Korenix JetWave 2610 Series

IEEE802.11a Wireless Outdoor AP/Bridge

User Manual

Version 2.1.9, Oct, 2009

www.korenix.com

Copyright

Copyright © 2009 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual is intended to guide professional installer to install the R1 Extender and how to build the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

Note:

- This indicates an important note that you must pay attention to.

Warning:

- This indicates a warning or caution that you have to abide.

Bold: Indicates the function, important words, and so on.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall beep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Warranty

Z-Com's standard hardware warranty is for two (2) year from date of shipment from Z-Com or a Z-Com Distributor. Z-Com warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

IN NO EVENT SHALL Z-COM, INC. BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE RISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF Z-COM, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL Z-COM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Content

Chapter 1 Introduction 12

Introduction 12

Appearance 12

Key Features 13

Typical Applications 14

Telemedicine Wireless Broadband Application 14

Education Wireless Broadband Application 15

Chapter 2 Hardware Installation 16

Preparation before Installation 16

Professional Installation Required 16

Safety Precautions 17

Installation Precautions 17

Product Package 18

Hardware Installation 20

Assemble the Mounting Bracket 20

Pole Mounting 20

Interface Definition 22

Connect Up 24

Grounding 25

Power On 26

Chapter 3 Basic Settings 28

Factory Default Settings 28

System Requirements 29

How to Login the Web-based Interface 30

Basic System Setup 32

Basic Wireless Settings 33

Chapter 4 Advanced Settings 36

Advanced Wireless Settings 36
Peer-to-Peer Links 38
Antenna Alignment Tool 40
Link Test 41
Super Mode 42
Wireless Security Settings 44
Security Profile Configuration 44
Access Control 46
RADIUS Settings 47

Chapter 5 Management 49

View R1 Extender Basic Information 49
View Ethernet Statistics 50
View Wireless Statistics 51
Connection 52
Password 53
Remote Management 54
Remote Console 54
SNMP 57
Time Settings 59
GPS Coordinate Settings 59
Upgrade Firmware 60
Backup/Restore Settings 62
Restore Factory Default Settings 63
Event Log 64
Reboot 65

Chapter 6 Troubleshooting 66

Appendix A. Channel – Frequency Table 68

Appendix B. Channel – Country List Table 70

Appendix C. ASCII 74

Appendix D. SSH Settings..... 75

Appendix E. GPL Declamation..... 80

FIGURE

Figure 1 R1 Extender 12

Figure 2 Telemedicine Wireless Broadband 14

Figure 3 Campus Wireless Broadband 15

Figure 4 Bracket Mounting – Step 1 20

Figure 5 Bracket Mounting – Step 2 20

Figure 6 Pole Mounting –Step 1 21

Figure 7 Pole Mounting – Step 2 21

Figure 8 Pole Mounting – Step 3 21

Figure 10 Detailed View of RS-232 Port 23

Figure 11 Warning Label 23

Figure 12 Vent 24

Figure 13 Connect Up – Step 1 24

Figure 14 Connect Up – Step 2 25

Figure 15 Connect Up – Step 3 25

Figure 16 Connect Up – Step 4 25

Figure 17 Grounding 25

Figure 18 PoE Connection 26

Figure 19 Security Alert 30

Figure 20 Login 30

Figure 22 Basic Setup 32

Figure 23 Basic Wireless Settings 33

Figure 24 Advanced Parameters 36

Figure 25 Peer-to-Peer Links for CSMA 38

Figure 26 PTP/PTMP for TDMA 39

Figure 27 Antenna Alignment Tool 40

Figure 28 Link Test 41

Figure 29 Super Mode 42

Figure 30 Security 44

Figure 31 Access Control 46

Figure 33 Basic Information 49

Figure 34 Ethernet Statistics 50
Figure 35 Wireless Statistics 51
Figure 36 Connection 52
Figure 37 Password 53
Figure 38 Remote Management 54
Figure 39 PuTTY Configuration 1 55
Figure 40 PuTTY Configuration 2 56
Figure 41 SSH 57
Figure 42 Obtain MIB File 58
Figure 43 Time Settings 59
Figure 44 Upgrade Firmware 61
Figure 45 Backup/Restore Settings 62
Figure 46 Restore Settings 63
Figure 47 Event Log 64
Figure 48 Reboot 65

TABLE

Table 1 PIN Definition 22

Table 3 RSSI-Beep Frequency 41

Table 4 Channels in 5MHz Centre Frequency 68

Table 5 Channels in 10MHz Centre Frequency 68

Table 6 Channels in 20MHz Centre Frequency 69

Table 7 Channels in 40MHz Centre Frequency 69

Table 8 Country of FCC 70

Table 9 Country of European Union 71

Table 10 Other Countries 72

Table 11 ACSII 74

Table 12 SSH Settings 75

Table 13 Public Software Name and Description 81

Chapter 1 Introduction

Introduction

Designed for outdoor environment application, the R1 Extender is a high-performance outdoor-deployable wireless bridge that provides wireless connectivity among multiple network locations. The R1 Extender has a built-in 23dBi planar antenna that can deliver up to a 40Km connection.

The R1 Extender is a multi function communication device that supports Base Station, CPE, PTP and PTMP connectivity. It allows for local area network (LANs) in different locations (buildings) to be easily interconnected. The R1 Extender delivers “last mile” broadband connectivity through its PTP and PTMP capabilities.

With high throughput and long-distance transmission, R1 Extender is an ideal backhaul solution for Carriers, Service Providers and Enterprises!

Appearance

Figure 1 R1 Extender

Key Features

- Provide easy installation and high performance wireless connectivity of up to 40km
- IP67 waterproof housing endures almost any harsh environments
- Multiple operating modes including Base station, CPE, PTP and PTMP
- Support 64/128-bit WEP and 802.1X, WPA-PSK, WPA2-PSK and WPA-PSK&WPA2-PSK, etc
- Support WMM and Quality of service (QoS) for enhanced performance
- Proprietary Antenna Alignment Tool helps identify the antenna orientation with the best signal strength
- Buzzer design helps to determine the device power initial condition
- Super mode to boost the data rate up to 108Mbps
- Advanced management tools like SNMP and Secure Shell (SSH)
- User-friendly Web, SSH and SNMP-based management interface

Typical Applications

This section describes the typical applications of the R1 Extender.

Telemedicine Wireless Broadband Application

The R1 Extender primary usage is as a relay or bridging technology that may be combined with cost effective solar power solution allowing for telemedicine application in remote and rural environments. The R1 Extender is able to deliver stable and high performance broadband connectivity for typical telemedicine applications in a Line-of-Sight environment.

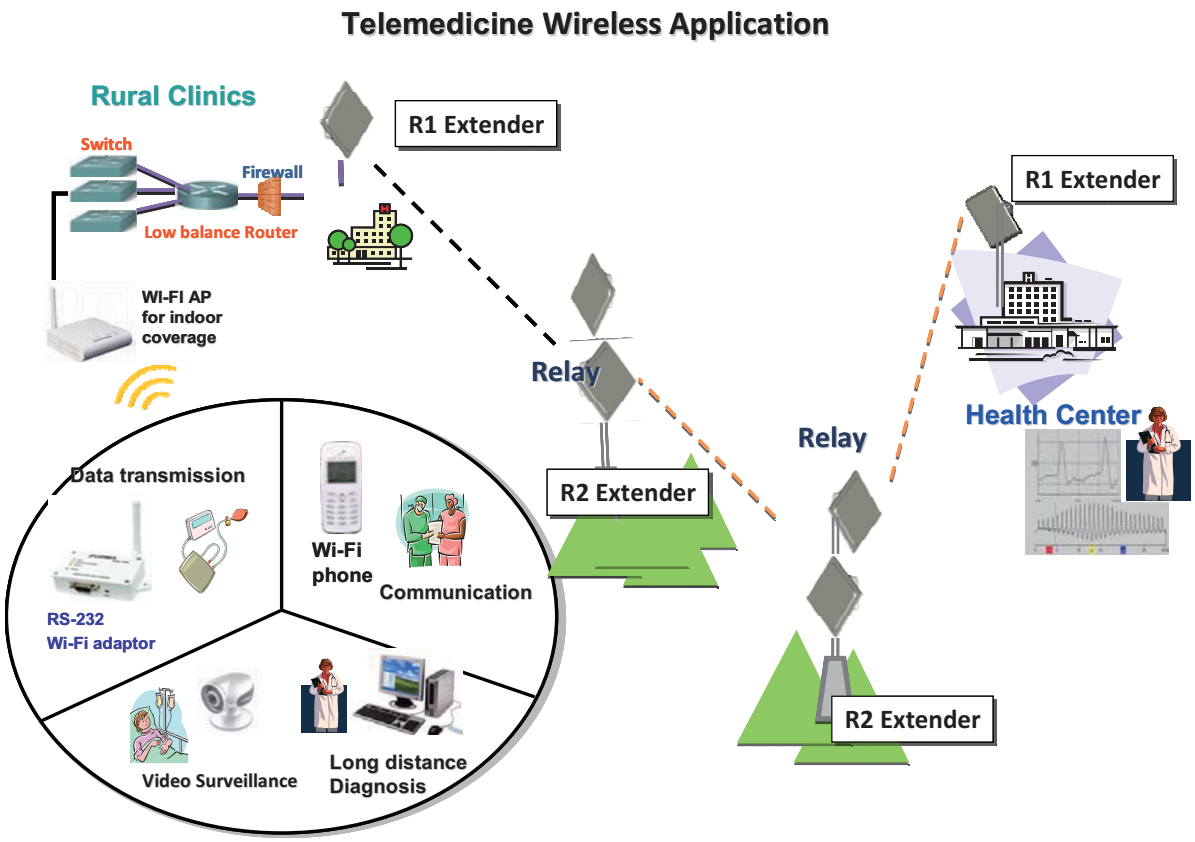


Figure 2 Telemedicine Wireless Broadband

Education Wireless Broadband Application

School in remote area or rural areas can be provided with broadband connectivity via local Internet service providers. The relay ability of the R1 Extender allows for multiple hops to be made thus allowing the R1 Extender to reach more remote LOS locations beyond 40km or to circumvent natural obstructions like mountains.

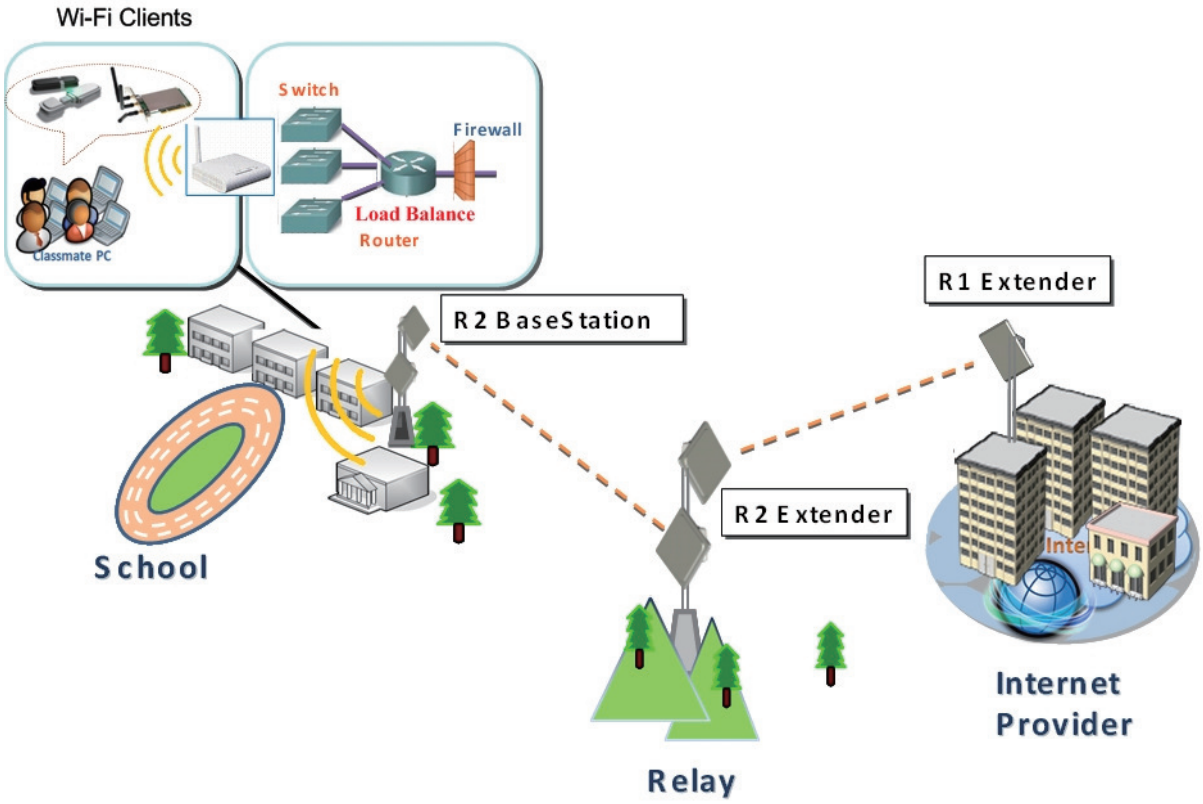


Figure 3 Campus Wireless Broadband

Besides, the R1 Extender can also be applied into the following environments:

- Cost-effectively provide long distance backhaul for remote areas (e.g. village, oil well, island, mountain and etc.)
- Establish local backhaul for campus, farm and factory
- Provide and access for video streaming or surveillance for industrial and mining enterprises
- Plays as a relay connecting different networks

Chapter 2 Hardware Installation

This chapter describes safety precautions and product information you have to know and check before installing R1 Extender.

Preparation before Installation

Professional Installation Required

1. Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.
2. The R1 Extender is distributed through distributor and system installer with professional technicians and will not be sold directly through retail store.
3. The equipment shall be installed in RESTRICTED ACCESS LOCATIONS. Access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken. Furthermore, access is through the use of a tool or lock and key, or other means of security, and is controlled b the authority responsible for the location.
4. If you are intended to use an external antenna with the R1 Extender, please contact your supplier/installer to ensure that your unit is set for you have fulfilled all the local regulatory requirements. It is the responsibility of the installer/user to check that the equipment as deployed meets local regulatory requirements.

Safety Precautions

To keep you safe and to install the hardware properly, please read and follow these safety precautions.

- ONLY qualified service personnel should service or disassemble this device;
- When installing the device, note the followings:
  - Do NOT use a metal ladder;
  - Do NOT work on a windy or raining day;
  - Do NOT install, use or service the device during a thunderstorm, as this may cause a remote risk of electric shock from lightning;
  - Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
  - When the system is operational, avoid standing directly in front of the antenna. Strong RF fields are present when the transmitter is on.
- Ground the device properly with grounding wire to protect against lightning;
- Use ONLY appropriate accessories for the device.
- If the temperatures of the unit surface exceeds the limit, be precautious not to continuous held or touch the device for a certain period of time.

Installation Precautions

To keep the R1 Extender well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed surge arrestor and grounding kit with R1 Extender; otherwise, a random lightening could easily cause fatal damage to R1 Extender. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.**
2. Make sure PoE is correctly connected to the RJ-45 port on the R1 Extender labeled PoE+Data. **DO NOT CONNECT TO THE PORT LABELED "Warning!! No POE"**, otherwise the extender will be severely damaged!

Product Package

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

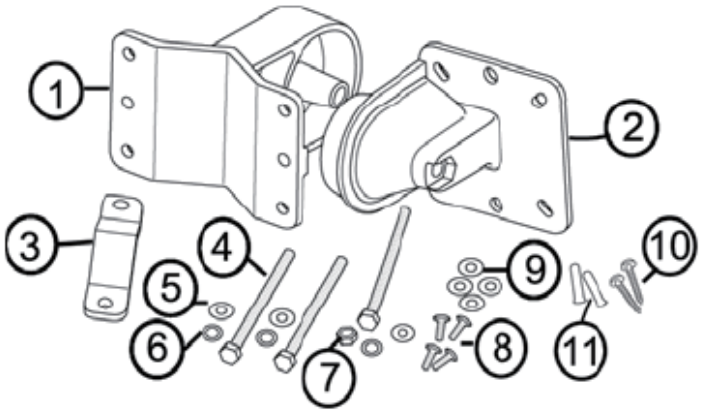
- R1 Extender with integrated 23dBi antenna ×1
- Mounting Kit ×1
- PoE Injector & Power cord ×1
- Grounding Wire with Screw ×1
- Waterproof RJ-45 Connector Kit ×1
- Quick Installation Guide ×1
- Product CD ×1

Note:

- Product CD contains Management Tool, Quick Installation Guide and User Manual!

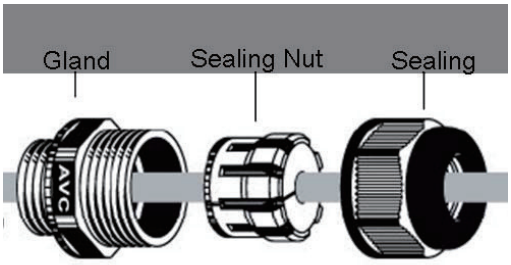
Mounting Kit

- **Wall/Pole Mounting Bracket**
  1. T-Form Bracket ×1
  2. Articulation Pole ×1
  3. Pole Mount Bar ×1
- **Fasteners**
  4. M8×80 Screw ×2
     M8×90 Screw ×1
  5. M8 Washer ×3
  6. M8 Spring Washer ×3
  7. M8 Nut ×1
  8. M5×16 Screw ×4
  9. M5 Washer ×4
  10. Wood Screw ×4 (for Wall Mount)
  11. Wall/Gyprock Plug ×4 (for Wall Mount)



Waterproof RJ-45 Connector Kit

1. Gland ×1
2. Sealing Nut ×1
3. Sealing ×1



Hardware Installation

Assemble the Mounting Bracket

1. Place the main bracket into the seating and use a spanner to fasten the bracket to the R1 Extender with M5×16 screws ⑧ and M5 washers ⑨ provided in the hardware packets;

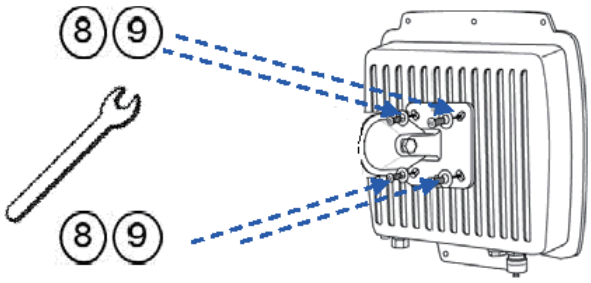


Figure 4 Bracket Mounting – Step 1

2. Assemble the main bracket by placing articulation pole ② to the T-form bracket ① via a M8×90 ④ screw through the insertion axe and fix with the M8 washer ⑤ , spring washer ⑥ and M8 nut⑦;

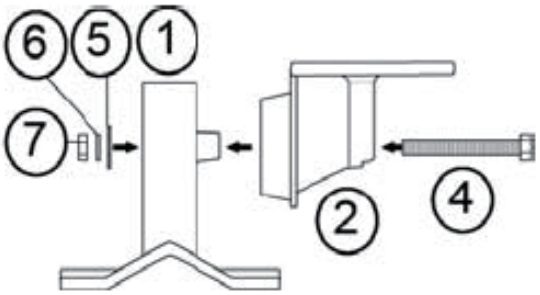


Figure 5 Bracket Mounting – Step 2

Pole Mounting

1. Install the main bracket and the pole mount bar ③ over the top of the pole by securing the drill holes of the pole mount bar to the main bracket ones and insert two M8×80 ④ screws, spring washers ⑥ and washers ⑤ through the drill holes and main bracket;

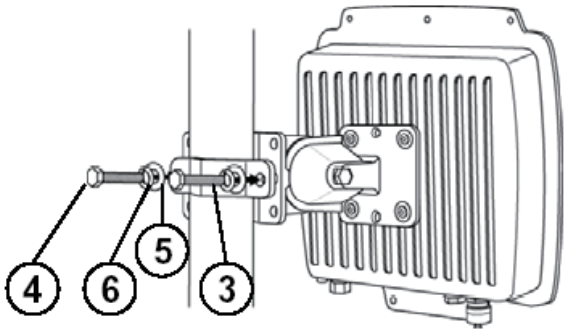


Figure 6 Pole Mounting –Step 1

2. Fasten two M8×80 screws ④ and washers ⑤ through the drill holes and main bracket with a spanner;

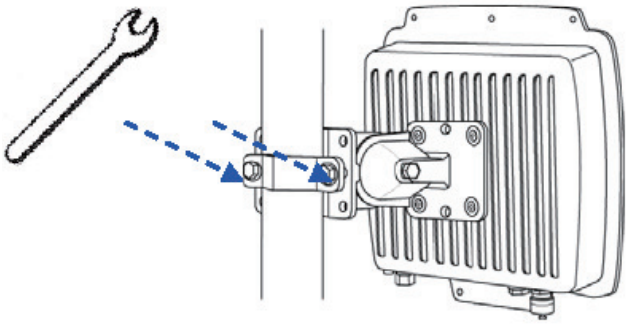


Figure 7 Pole Mounting – Step 2

3. Adjust the antenna for appropriate tilt / vertical orientation.

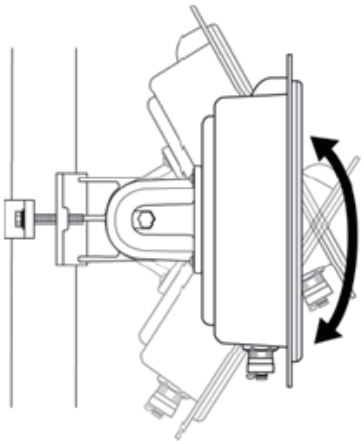


Figure 8 Pole Mounting – Step 3

Note:

- The horizontal and vertical beam width of R1 default antenna is about 10 degree respectively.

Interface Definition

The R1 Extender currently provides two interfaces at the bottom, which are PoE + Data with a black plastic cover and RS-232 with a light gray cover that label "**WARNING! No PoE**". Among which, a black RJ45 waterproof connector will be provided for the PoE + Data interface.

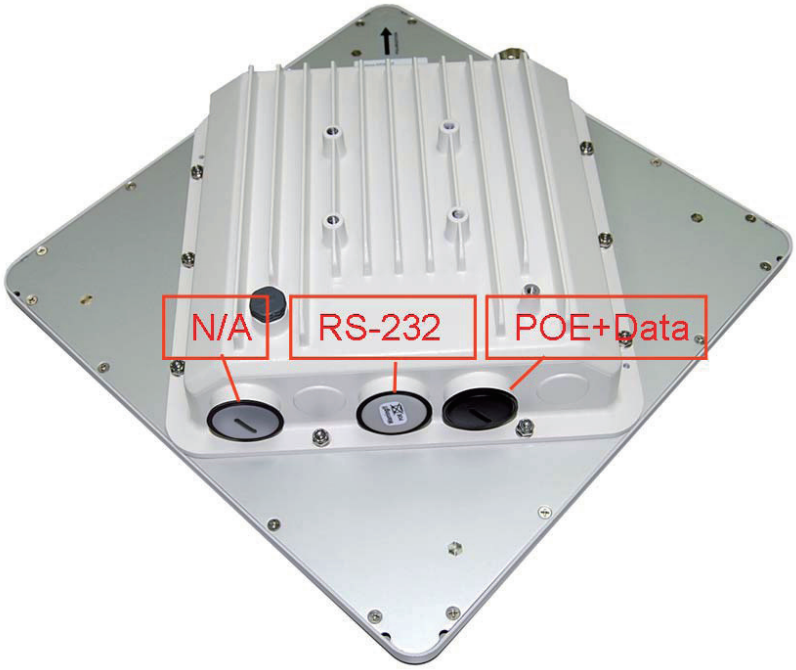


Figure 9 Interface Definition

RS-232

RS-232, which is labeled **COM/RESET**, is used for debugging purposes as well as for hard reset of the R1 Extender. Below you may find the pin definition of the RS-232.

Table 1 PIN Definition

Pin Assignment	Name	Description
P1	TXD0	Data Transmit 0
P2	DSR0	Data Set Ready 0
P3	RXD0	Data Receive 0
P4	TXD1	Data Transmit 1
P5	RXD1	Data Receive 1
P6	DTR1	Data Terminal Ready
P7	Hard Reset	Hard reset the unit
P8	GND	Ground

To reset the device, short P7 (Hard Reset) to P8 (GND) for less than 1 second and the system will reset. If P7 (Hard Reset) is shorted to P8 (GND) for over 5 seconds, the R1 Extender will be reset to the factory default settings.

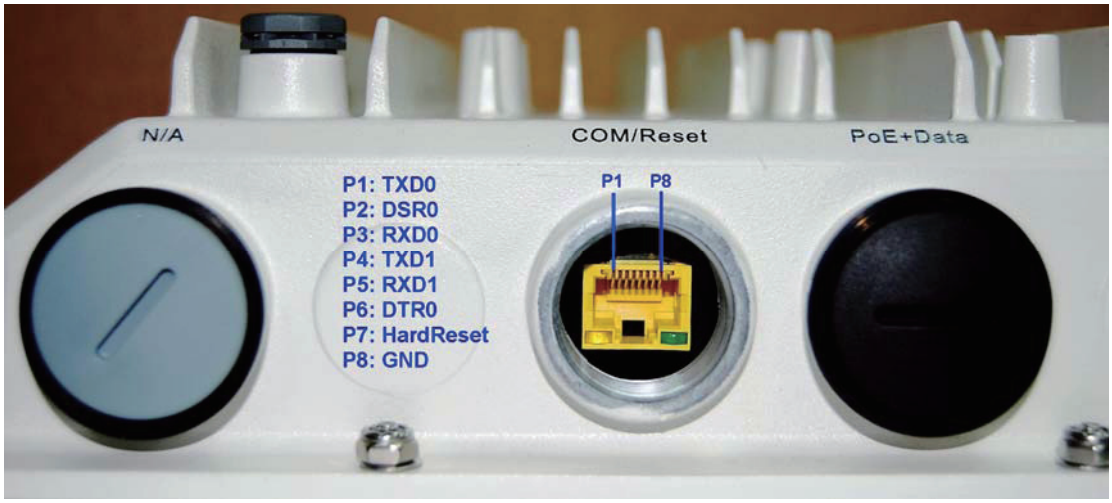


Figure 10 Detailed View of RS-232 Port

Below are the views of RS-232 cover and RJ-45 port respectively, please note the label covered on and DO strictly follow the instructions to avoid damaging your equipment!

Figure 11 Warning Label

Warning:

- Do NOT connect PoE powered Ethernet cable to the RS-232 port; otherwise the port may burnout!
- If RS-232 cable is used outdoor, please DO add a surge protector to protect the equipment circuit!
- Strongly recommend to add a lightning arrestor on the RS-232 port to prevent from lightning attack!

Vent

The vent is designed to exclude vapors and moisture out of the unit as well as repel water, dust, and dirt by the specially designed membrane, thereby preventing the R1 Extender from electric malfunctioning.

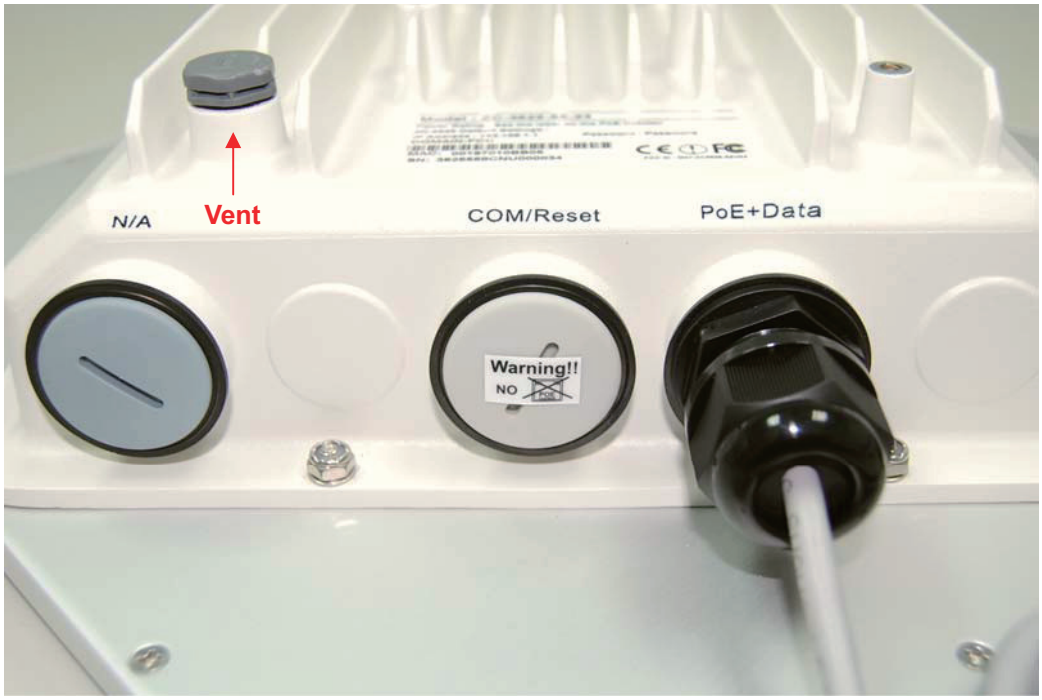


Figure 12 Vent

Connect Up

Before installing the Ethernet cable with a waterproof RJ-45 connector, it is recommended that the Cat-5 RJ-45 coaxial cable be used for the R1 Extender to power PoE connector.

1. To connect to the hole labeled **PoE+Data**, open the black cover in advance by using a coin or a slotted screwdriver and then screw in the body of the gland and tighten.

Figure 13 Connect Up – Step 1

2. Slide the sealing nut to the RJ-45 cable from its middle breach and then insert the sealing into the cable.

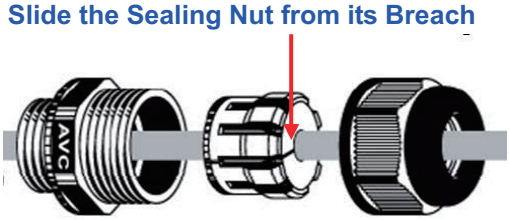
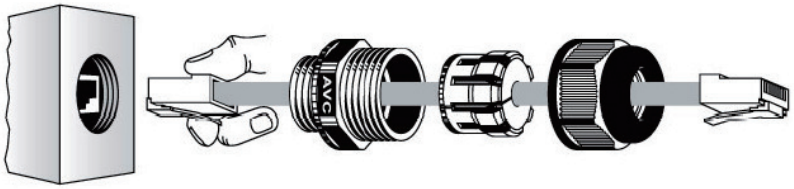


Figure 14 Connect Up – Step 2

3. Insert the RJ-45 connector and make sure that the locking tab snaps home.



R1 Extender RJ-45 Port

Figure 15 Connect Up – Step 3

4. Screw the sealing on the gland and tighten.

Figure 16 Connect Up – Step 4

Grounding

The R1 Extender is shipped with a grounding wire. The unit must be properly grounded to protect against power surges. The grounding point can be found on the bottom of the unit. It is supplied with an appropriate grounding lug for attachment to the ODU.

Figure 17 Grounding

Power On

To power up the R1 Extender, follow the steps bellow:

1. Plug a user-supplied Cat-5 Ethernet cable from your wired LAN (or a computer) into the power injector RJ-45 jack (**DATA IN**);
2. Plug a user-supplied Cat-5 Ethernet cable from the R1 Extender into the power injector RJ-45 jack (**P+DATA OUT**);
3. Connect the power module to the power injector and plug the AC cord into an AC power receptacle;
4. After being powered on, the device will send out the beep sound lasting about 1.5 seconds, informing you that the R1 Extender is powered up! Wait about 60 seconds the system will be initialized and start working.

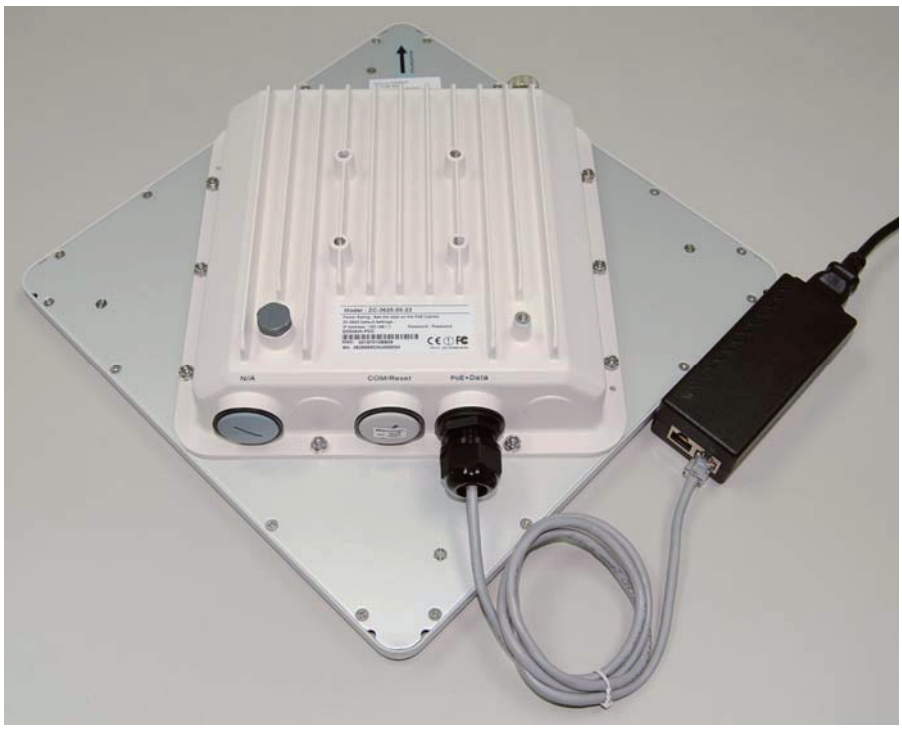


Figure 18 PoE Connection

Warning:

- Make sure PoE is correctly connected to the RJ-45 port on the R1 Extender labeled PoE+Data, otherwise the extender will be severely damaged!

N/A
COM/Reset
PoE+Data
Warning!!
NO

Chapter 3 Basic Settings

Factory Default Settings

We'll elaborate the R1 Extender factory default settings. You can re-acquire these parameters by default. If necessary, please refer to the "Restore Factory Default Settings".

Table 2 R1 Extender Factory Default Settings

Features		Factory Default Settings
Username		admin
Password		password
Wireless Device Name		DEVICEXXXXXX (X represents the last 6 digits of Ethernet MAC address)
Operating Mode		Peer-to-Peer (CSMA)
Country/Region		United States (Country dependent and software programmed)
Ethernet Data Rate		Automatic
LAN	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Gateway	0.0.0.0
	Primary DNS Server	0.0.0.0
	Secondary DNS Server	0.0.0.0
DHCP Client		Disable
Spanning Tree		Enable
Wireless Mode		802.11a
Channel/Frequency		149/5.745GHz (CE: 100/5.5GHz)
BSSID		wireless
Transmit Rate		Best
Output Power		100% (Full)
Bandwidth		20MHz
TDM Coordination		Disable
WMM		Disable
Super Mode		Disable
RTS Threshold (byte)		2346
Fragmentation Length (byte)		2346
Beacon Interval		100
Distance in Meters		10000
Security		Open System
Encryption		None

Wireless Client Isolation		Disable
Access Control		Disable
SSH (Secure Shell)		Enable
SNMP	Enable/Disable	Enable
	Read Community Name	Public
	Write Community Name	Private
	IP Address	0.0.0.0

System Requirements

Before configuration, please make sure your system meets the following requirements:

- A computer coupled with 10/ 100 Base-TX adapter;
- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of R1 Extender is 192.168.1.1, X can not be 0, 1, nor 255;
- A Web browser on PC for configuration such as Microsoft Internet Explorer 6.0 or above, Netscape or Firefox.

How to Login the Web-based Interface

The R1 Extender provides you with user-friendly Web-based management tool.

- Open IE and enter the default IP address (Default: **192.168.1.1**) of R1 Extender into the address field. A Security Alert window may popup as below, due to browser's security trusted sites. You may choose to continue to the login webpage.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No
View Certificate

Figure 19 Security Alert

- Click "**Yes**" will usher you into the login page:

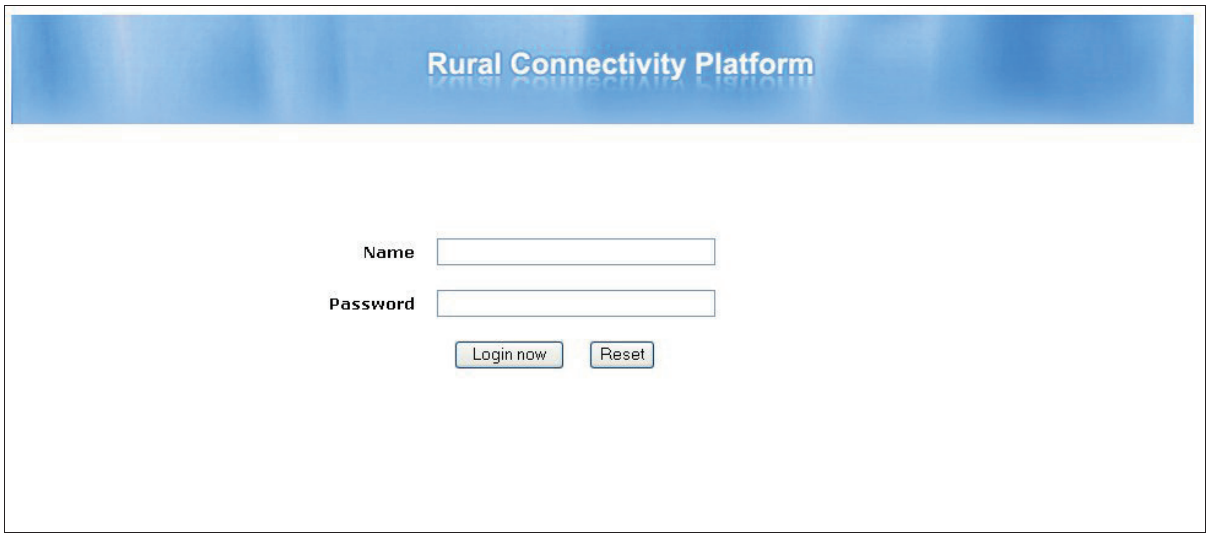


Figure 20 Login

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click "**Login Now**" to login the main page of R1 Extender. As you can see, this management interface provides four main options in the black bar above, which are System, Wireless, Status and Management.

Figure 21 Main Page

Note:

- The username and password are case-sensitive, and the password is no more than 19 characters!

Basic System Setup

For users who use this device for the first time, it is recommended that you begin configuration from "**Basic**" in "**System**" shown below:

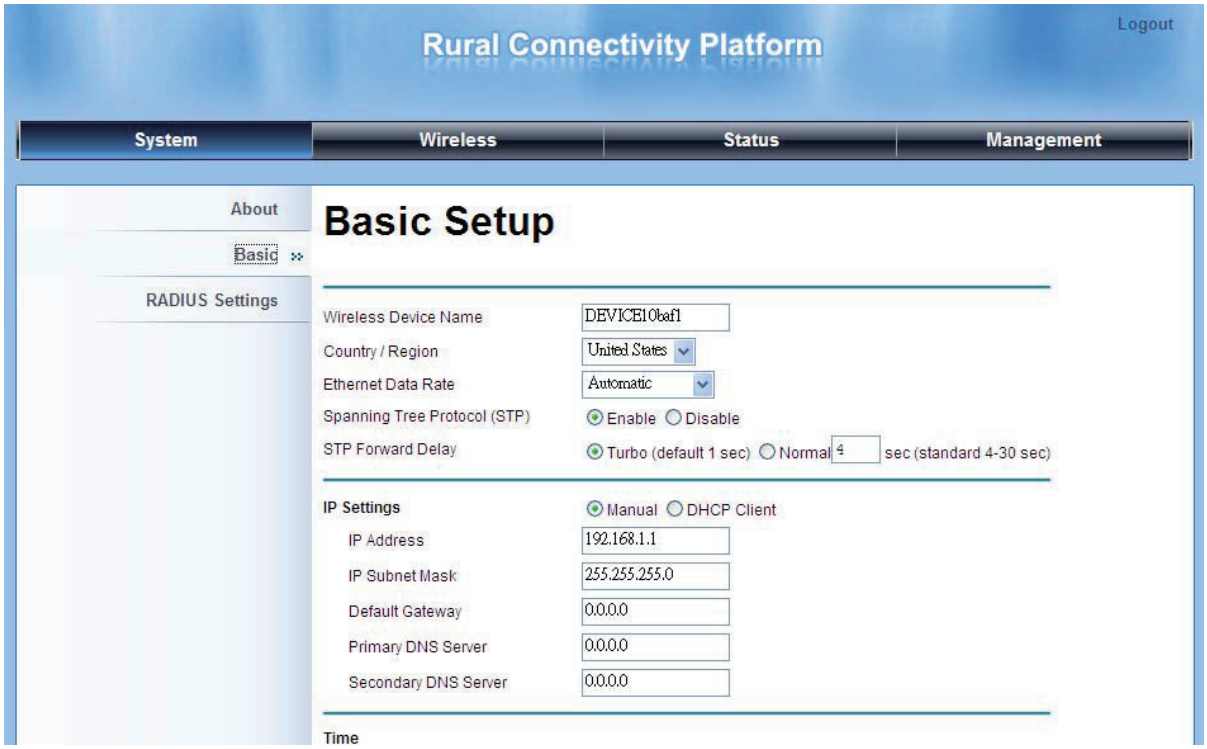


Figure 22 Basic Setup

- **Wireless Device Name**

  Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

- **Country/Region**

  For the available radio bands vary from country to country, the working channels used are different.

- **Ethernet Data rate**

  Specify the transmission rate of data.

- **IP Address**

  If you select "**Manual**", you have to specify a static IP address, subnet mask, default gateway and DNS server for your local area network which connects to the LAN port of R1 Extender. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

- **DHCP Client**

  Enable DHCP client to allow the DHCP server within your local area network to assign an IP

address automatically.

- **Spanning Tree Protocol (STP)**

  Spanning Tree Protocol is a link management protocol for RCP bridges which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the RCP bridges but establish the redundant link as a backup if the initial link fails.

- **STP Forward Delay**

  STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec. Select Normal if you would like to modify the parameter (4-30 seconds).

Basic Wireless Settings

Open "**Radio**" in "**Wireless**" as below to make basic wireless configuration.

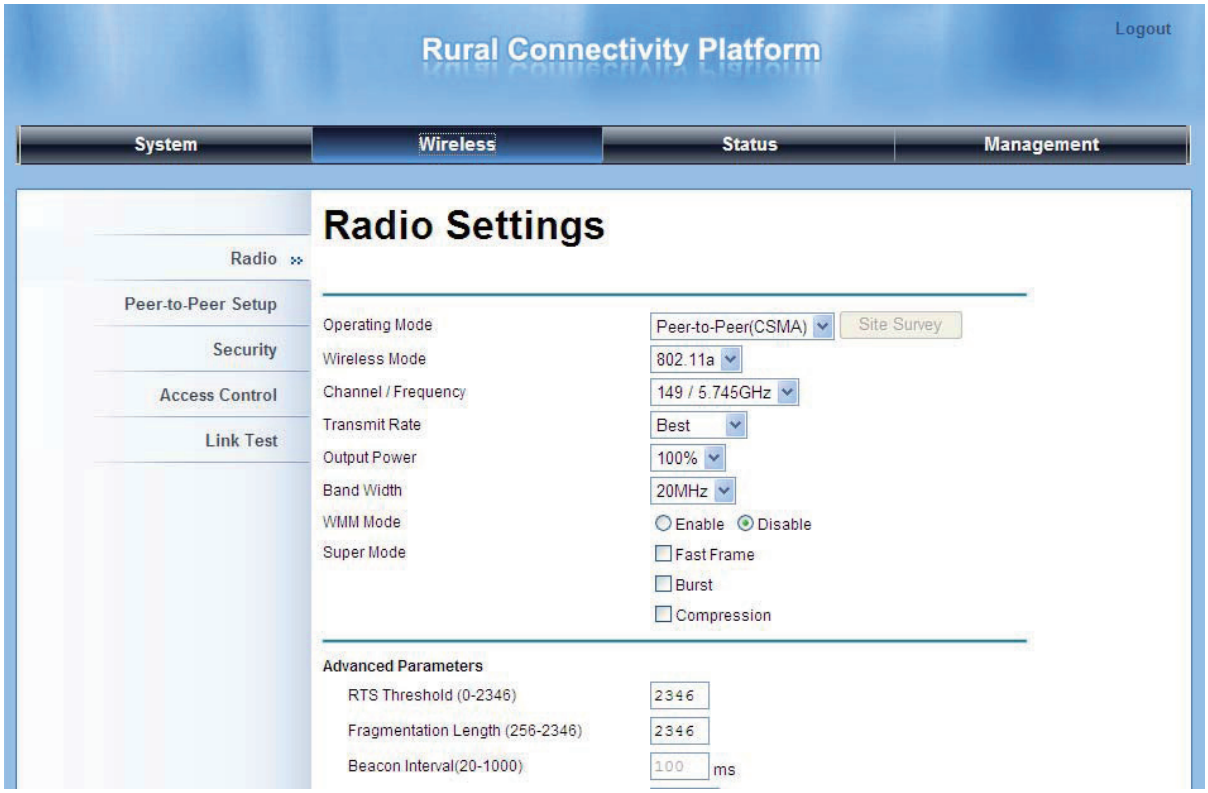


Figure 23 Basic Wireless Settings

- **Operating Mode**

  Four operating modes are available on R1 Extender. In a point to point environment where there are only two radios, Peer to Peer is recommended as it works more efficiently.

  Base Station: The R1 Extender connects directly to the main Ethernet LAN and receives connectivity from other wireless devices.

CPE: The R1 Extender connects to a remote LAN and the Base Station in it.

Peer-to-Peer (CSMA): The R1 Extender connects to another wireless device within the same networking program using CSMA protocol. CSMA ensures that only one node is transmitting on the network at any one time. Under this mode, both PTP and PTMP are available. It is highly recommended to use this mode when the distance between two nodes is less than 20km.

Peer-to-Peer (TDMA): The R1 Extender connects to another wireless device within the same networking program using TDMA protocol. TDMA divides each cellular channel into multiple time slots to increase the amount of data that can be carried; hence increase the throughput. Under this mode, only PTP is available and is suggested to use when the distance between the two R1 Extenders is greater than 20km.

- **Base Station ID (SSID)**

  For Base Station mode, it requires SSID for CPU clients to associate with. This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

- **Wireless Mode**

  The R1 Extender can only communicate with wireless devices of 802.11a.

- **Channel/Frequency**

  Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Transmit Rate**

  Usually "**Best**" is preferred. Under this rate, the R1 Extender will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Output Power**

  Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly then. Usually "**100%**" is preferred.

- **Band Width**

  Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. Among them, 40MHz can enhance the data rate more effectively, but will take more bandwidth, thus cause possible interference.

- **TDM Coordination**

Stands for “Time-Division Multiplexing technique”, this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in CSMA BS and CPE mode. Enable this function on both BS and CPE devices. It is highly recommended to enable TDM coordination when there are multiple CPEs needed to connect to the BS in your application.

- **NoACK**

  Under TDMA mode, enabling NoACK can enhance throughput but it might result in higher error rates in a noisy environment.

- **WMM**

  WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should support it as well.

- **Super Mode**

  Super mode is an effective way to enhance performance. It can boost the transmission data rate up to 108Mbps. The R1 Extender provides you with three kinds of Super mode, which are Fast Frame, Burst and Compression. To enable Super Mode, the remote R1 Extender should enable the function as well. For more information you may refer to Super Mode in **Chapter 4 Advanced Settings**.

Chapter 4 Advanced Settings

Advanced Wireless Settings

Open “**Radio**” in “**Wireless**” and turn to “**Advanced Parameters**” at the bottom to make advanced wireless settings.

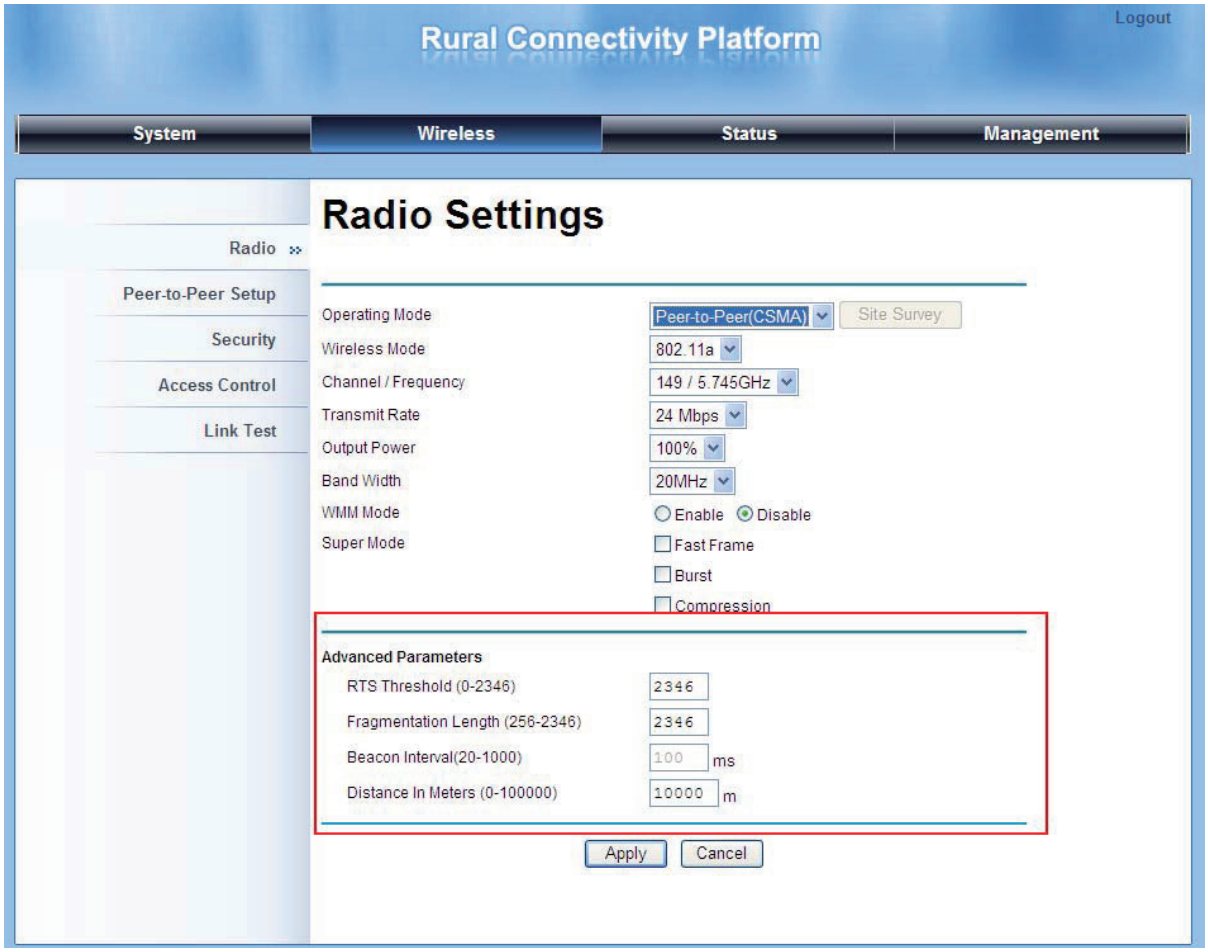


Figure 24 Advanced Parameters

- **RTS Threshold**

  The R1 Extender sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte.

- **Fragmentation Length**

  Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

  Specify the frequency interval to broadcast packets. Enter a value between 20 and 1000.

- **Distance in Meters**

  To decrease the chances of data retransmission at long distance, R1 Extender can auto adjust proper ACK timeout value by specifying distance of the two nodes. Default distance is 10Km. This is only useful for CSMA mode.

- **TDM Coordination Time Slice**

  Specify the time slice of TDM Coordination. It allows a certain amount of time (in ms) that data will transmit to each other before it moves to the next user. This is a repetitive cycle.

Note:

- We strongly recommended you leave most advanced settings at their defaults except Distance in Meters; any modification on them may negatively impact the performance of your wireless network.

Peer-to-Peer Links

Open “**Peer-to-Peer Setup**” in “**Wireless**”. Peer-to-Peer Links allow establishing PTP or PTMP connectivity with as most four remote wireless devices, this feature only available under Peer-to-Peer (CSMA) mode.

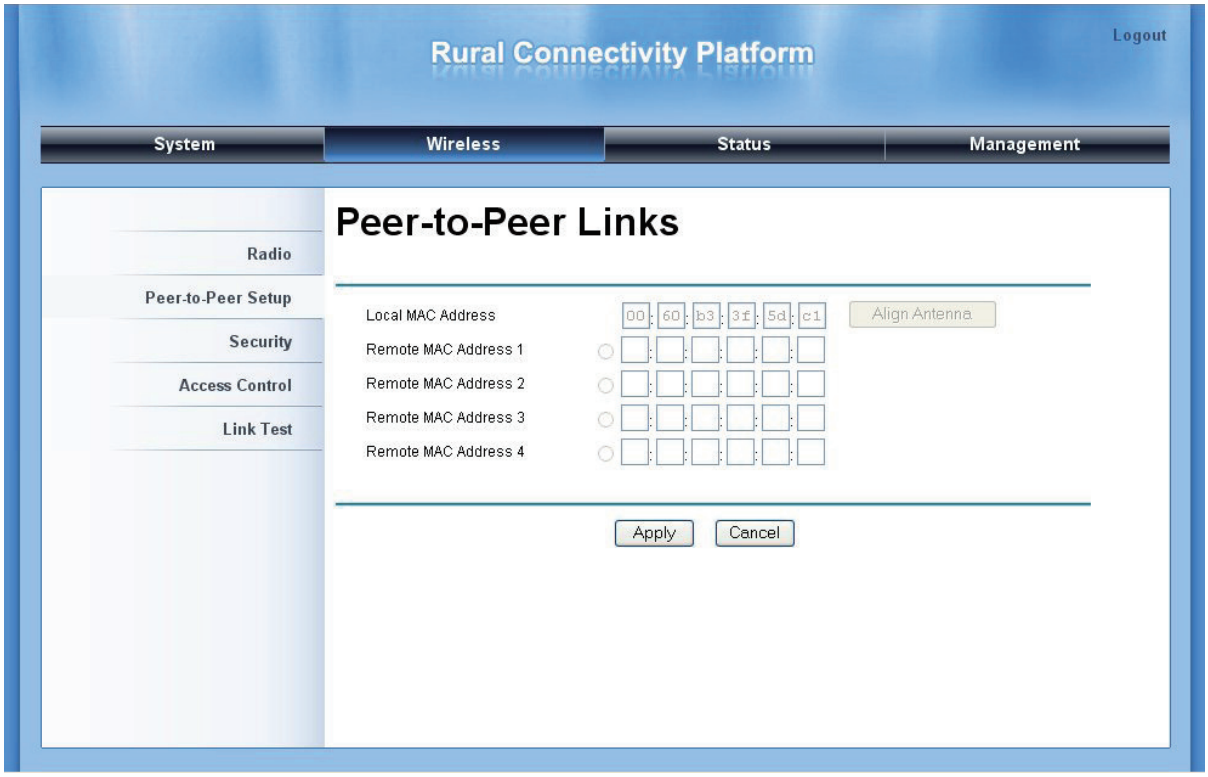


Figure 25 Peer-to-Peer Links for CSMA

- To setup Peer-to-Peer link, first login the Web-based interface of remote R1 Extender, open “**About**” in “**System**” and record the wireless MAC address of it.
- Then, login the Web-based interface of local R1 Extender and open “**Peer-to-Peer Setup**” in “**Wireless**”, input the WLAN MAC address of the remote one to “**Remote MAC Address 1**” field and click “**Apply**”;
- To check whether the link has been successfully established, you may use ping to justify.

The other way to establish PTMP connectivity is to setup the same group id under "**Radio**" in "**Wireless**". This feature only available under Peer-to-Peer (TDMA) mode and only devices with the same Group ID can communicate.

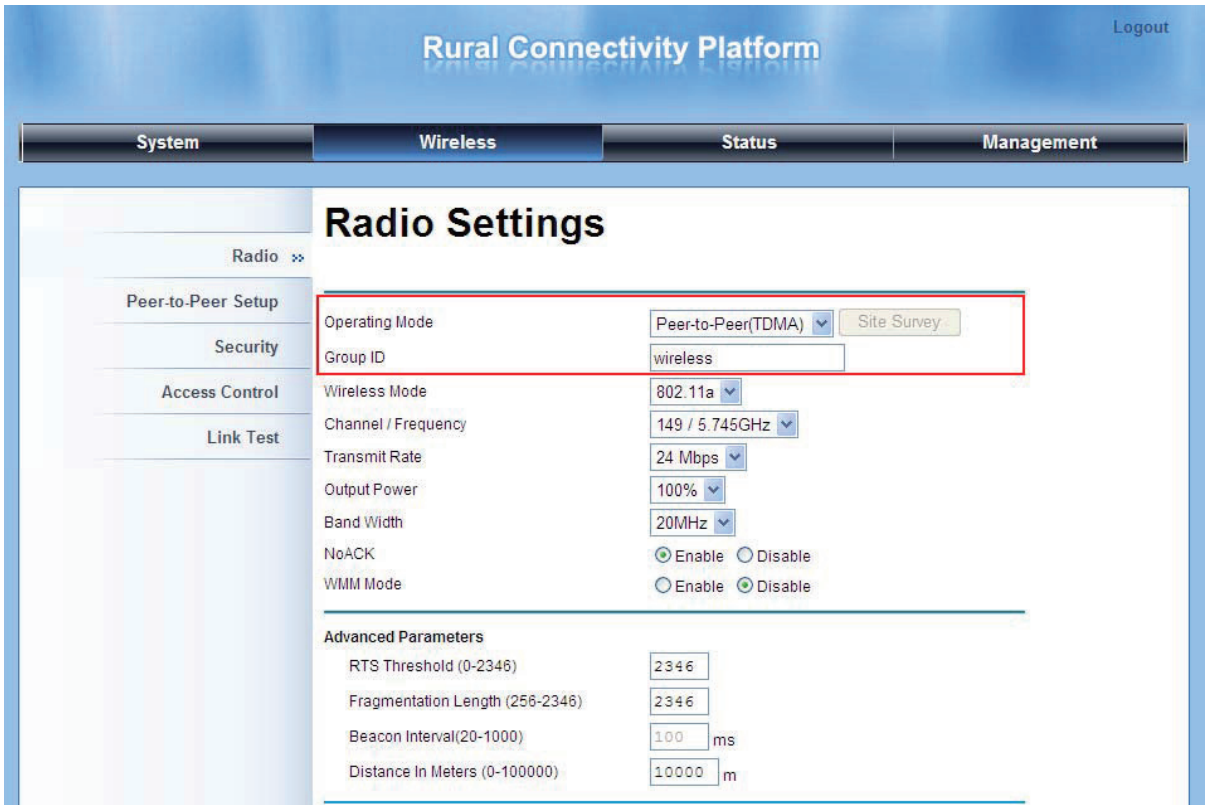


Figure 26 PTP/PTMP for TDMA

Note:

- When establish PTMP network, make sure all the remote wireless devices are within the antenna beam width.

Antenna Alignment Tool

Under Peer-to-Peer (CSMA) mode, Antenna Alignment Tool is available. This function helps to point in the approximate direction of the remote R1 Extender antenna and assist user easily align the local antenna to reach maximum signal strength.

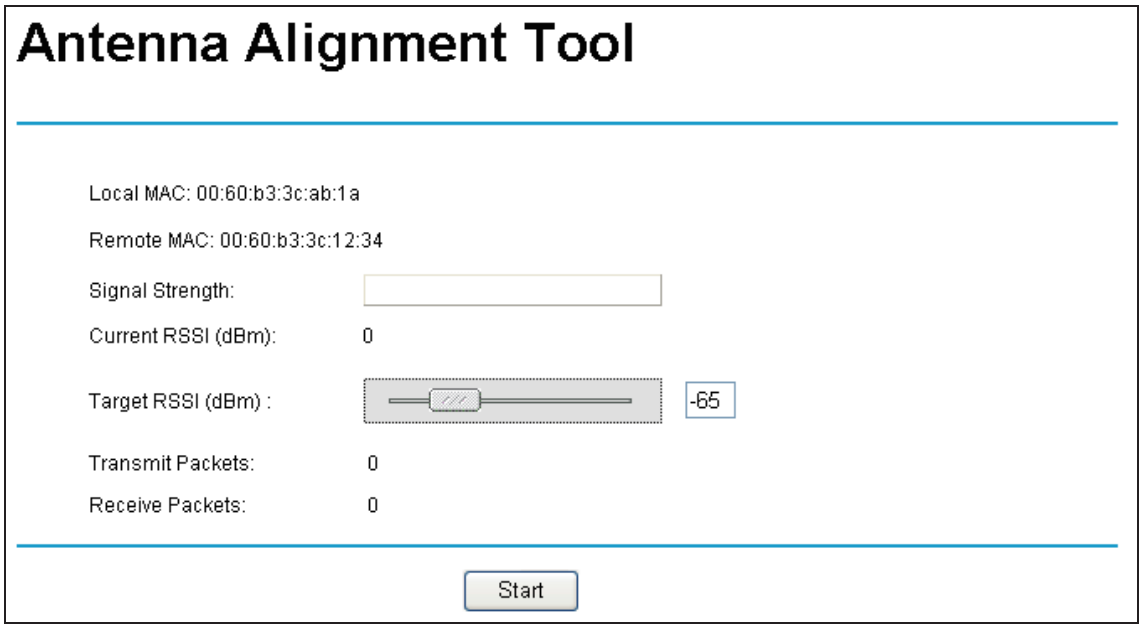


Figure 27 Antenna Alignment Tool

To use "**Antenna Alignment Tool**", follow the steps bellow:

- Open "**Peer-to-Peer Setup**" and select "**RF1**" or "**RF2**". Enter the MAC address of the remote bridge and click on the **Apply** button. Then click the "**Align Antenna**" button and the "**Antenna Alignment Tool**" window will popup.
- Set the target RSSI (e.g. -70dBm) and click "**Start**" button.
- Wait about 5 seconds, the antenna alignment starts and performs alignment every one second.
- Fix the local antenna and adjust the remote antenna elevation and horizontal direction. During the adjustment, observe "**Current RSSI**" in local R1 Extender. The value will refresh every 1 second. Fix the remote antenna when it reaches your expectation. Usually, RSSI between -60 and -70dBm indicates rather good signal strength.
- Adjust the local antenna after fixing the remote one. During the adjustment, observe "**Current RSSI**" in the remote R1 Extender. Fix the local antenna when it reaches your expectation.
- During the antenna alignment, the R1 Extender will issue beep sound to indicate current RSSI. Frequency of beep indicate the following RSSI:

Table 3 RSSI-Beep Frequency

RSSI	Beep Frequency
>-50	100 /sec
-50~-60	50 /sec
-60~-70	5 /sec
-70~-80	2 / sec
-80~-90	1 /sec
< -90	No beep sound

Link Test

Under Base Station, CPE or Peer-to-Peer (TDMA) mode when Antenna Alignment Tool is not available, Link Test provides another option to check the signal strength towards the connecting device. Open "**Link Test**" in "**Wireless**" as below, and click "**Refresh**" to view the current signal strength of wireless connectivity. The table will be updated every 3 seconds. If the signal is not so good, align the antenna manually.

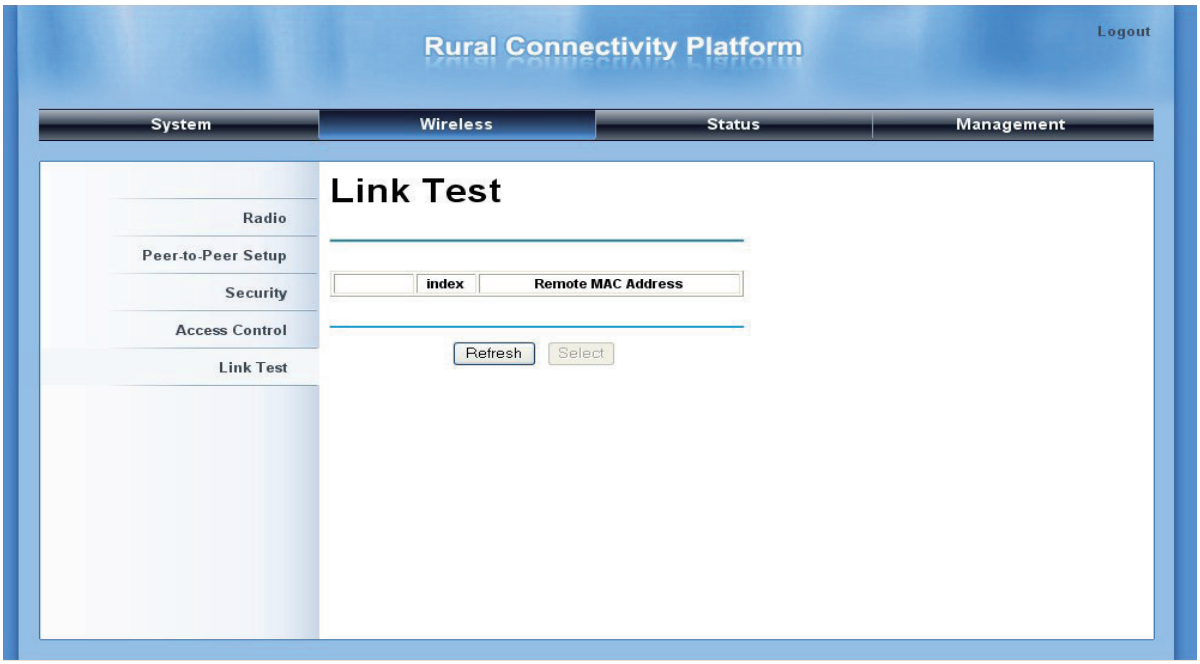


Figure 28 Link Test

Super Mode

Super mode is an effective way to enhance the Wi-Fi performance; it can boost the transmission data rate. R1 Extender provides you with three kinds of Super mode, which are Fast Frame, Burst and Compression.

Open "**Radio**" in "**Wireless**", Super Mode is in the red box as below:

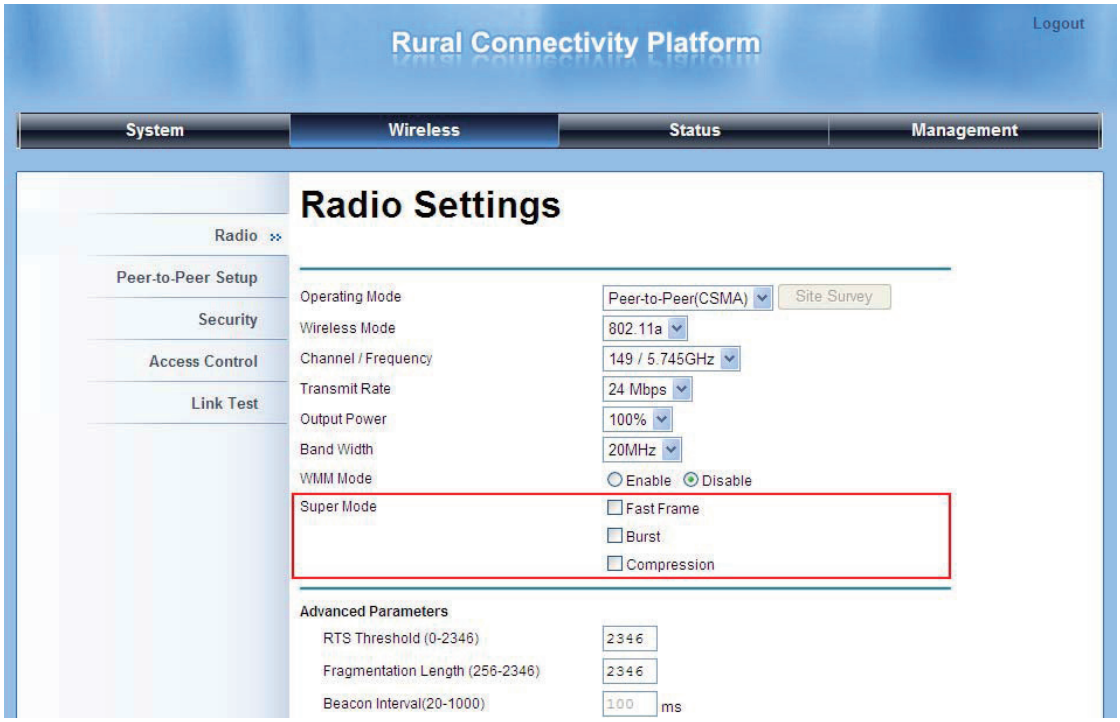


Figure 29 Super Mode

- **Fast Frame**

  By utilizing frame aggregation and timing modifications, it increases throughput via transmitting more data per frame and removing inter-frame pauses.

- **Burst**

  By allowing more data frames per given period of time, it increases throughput via overhead reduction.

- **Compression**

  By performing real-time hardware data compression, it increases throughput via using pre-compressed frames with no impact on host processor.

Note:

- Only all the wireless devices share the same wireless connectivity support Super mode, can this function be available!
- The throughput may vary depending on the actually environment and data traffic flow.

Wireless Security Settings

To prevent unauthorized radios from accessing data transmitting over the connectivity, R1 Extender provides you with rock solid security settings.

Security Profile Configuration

Open "**Security**" in "**Wireless**" as below:

Figure 30 Security

- **Broadcast SSID**

  Hiding network name is necessary when you are in a wireless environment that may have potential risk. By using this function, the STA can not scan and find R1 Extender, so that malicious attack by some illegal STA could be avoided.

- **Network Authentication**

  Open: It allows any device to join the network without performing any security check.

  Shared Key: Data encryption and key are required for wireless authentication before association. (Only available in BS and CPE mode).

  WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this

so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

  If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

  None: Available only when the authentication type is open system.

  64 bits WEP: It is made up of 10 hexadecimal numbers.

  128 bits WEP: It is made up of 26 hexadecimal numbers.

  152 bits WEP: It is made up of 32 hexadecimal numbers.

  TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

  AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

  TKIP + AES: It allows for backwards compatibility with devices using TKIP.

- **Wireless Client Isolation Mode**

  Enable this mode can prevent the communication between connected wireless clients.

Note:

- We strongly recommend you enable wireless security on your network!
- Only setting the same Authentication, Data Encryption and Key in the R1 Extender and other wireless devices that connecting with it, can the communication be established!

Access Control

The Access Control appoints the authority to STA on accessing R1 Extender, thus a further security mechanism is provided. This function is available only under Base Station mode.

Open “**Access Control**” in “**Wireless**” as below, check “**Turn Access Control On**” to enable this function.

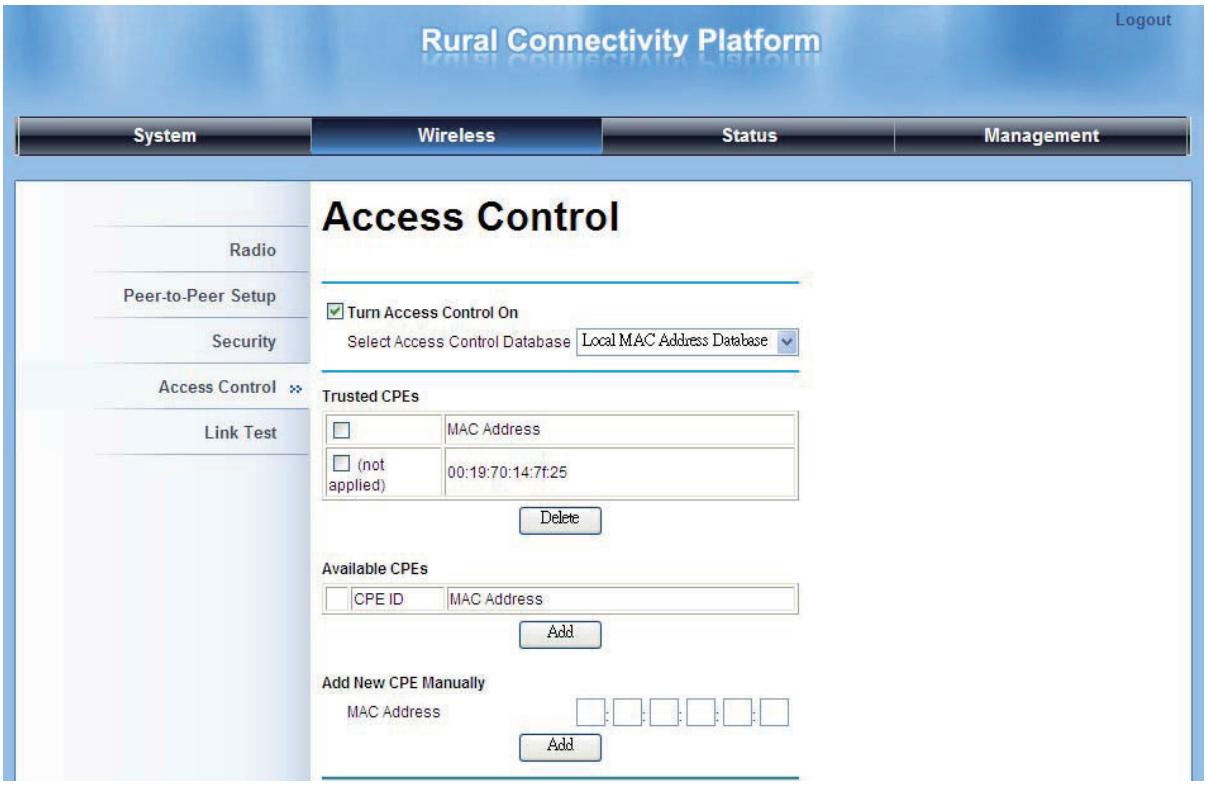


Figure 31 Access Control

- **Available CPEs**

  In this table lists the CPEs connecting with R1 Extender currently. Check the box before each MAC address, click “**Add**” to add one or more available CPE(s) into the “**Trusted CPEs**” and click “**Apply**” to save settings.

- **Add New CPE Manually**

  Enter the MAC address of the CPE that you would like to list into the access control list, click “**Add**” then the CPE will be added into the “**Trusted CPEs**”.

- **Trusted CPEs**

  Check the box before one or more MAC addresses of CPEs that you would like to cancel, and click “**Delete**” to cancel that access control rule.

RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share.

Open "**RADIUS Settings**" in "**System**" to make RADIUS configuration.

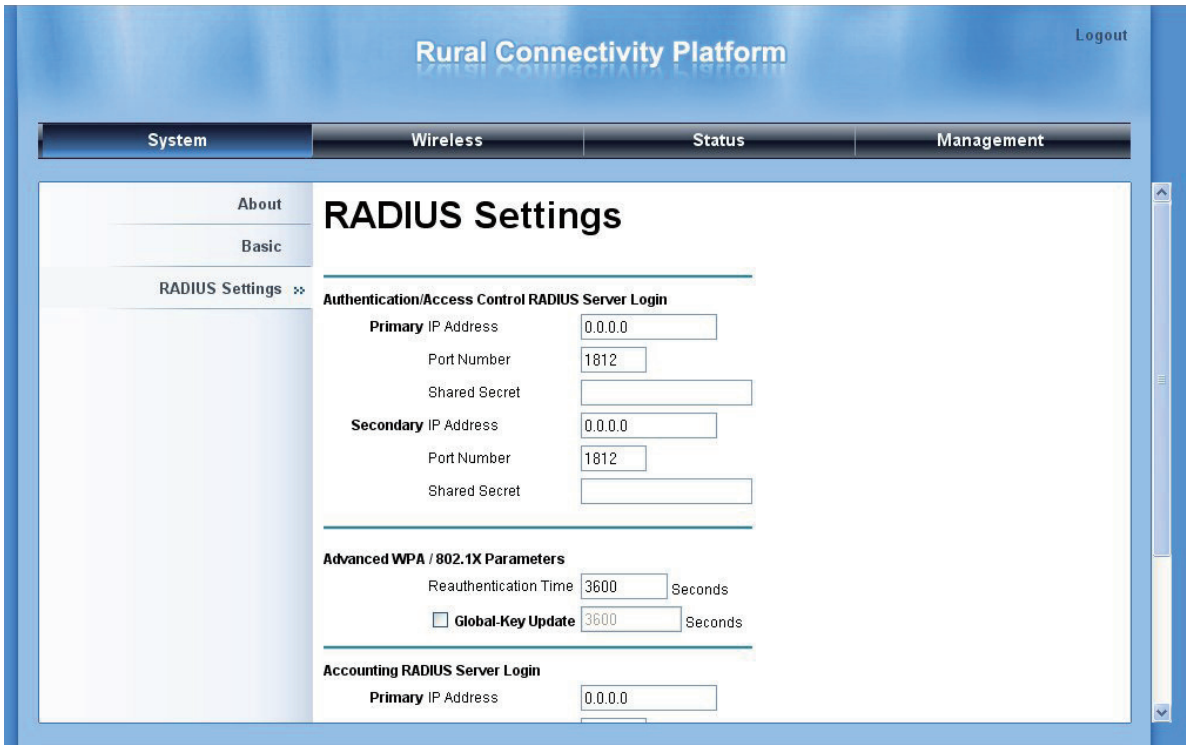


Figure 32 RADIUS Settings

- **Authentication/Access Control RADIUS Server Login**

  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port Number and Shared Secret. If the Primary RADIUS fails to work, the Secondary RADIUS Server is an option.

  IP Address: Enter the IP address of the Radius Server;

  Port Number: Enter the port number of the Radius Server;

  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the R1 Extender and RADIUS during authentication.

- **Advanced WPA/802.1X Parameters**

  Re-authentication Time: Set the time interval between two authentications.

  Global-Key Update: Check this option and specify the time interval between two global-key updates.

Chapter 5 Management

View R1 Extender Basic Information

Open “**About**” in “**System**” to check the basic information of R1 Extender, which is read only.

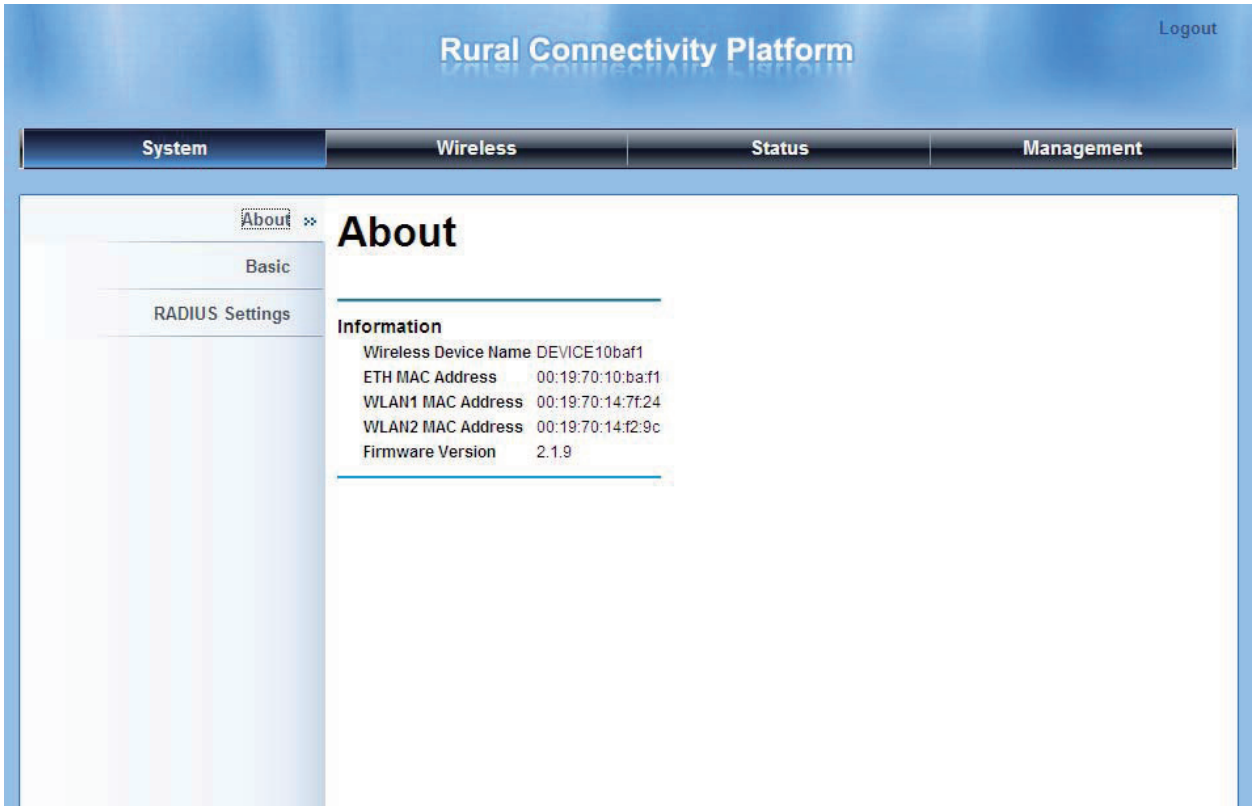


Figure 33 Basic Information

View Ethernet Statistics

Open “**Ethernet Status**” in “**Status**” to check the data packets received on and transmitted from the Ethernet port in LAN. Click “**Refresh**” to view current statistics. All is read only.

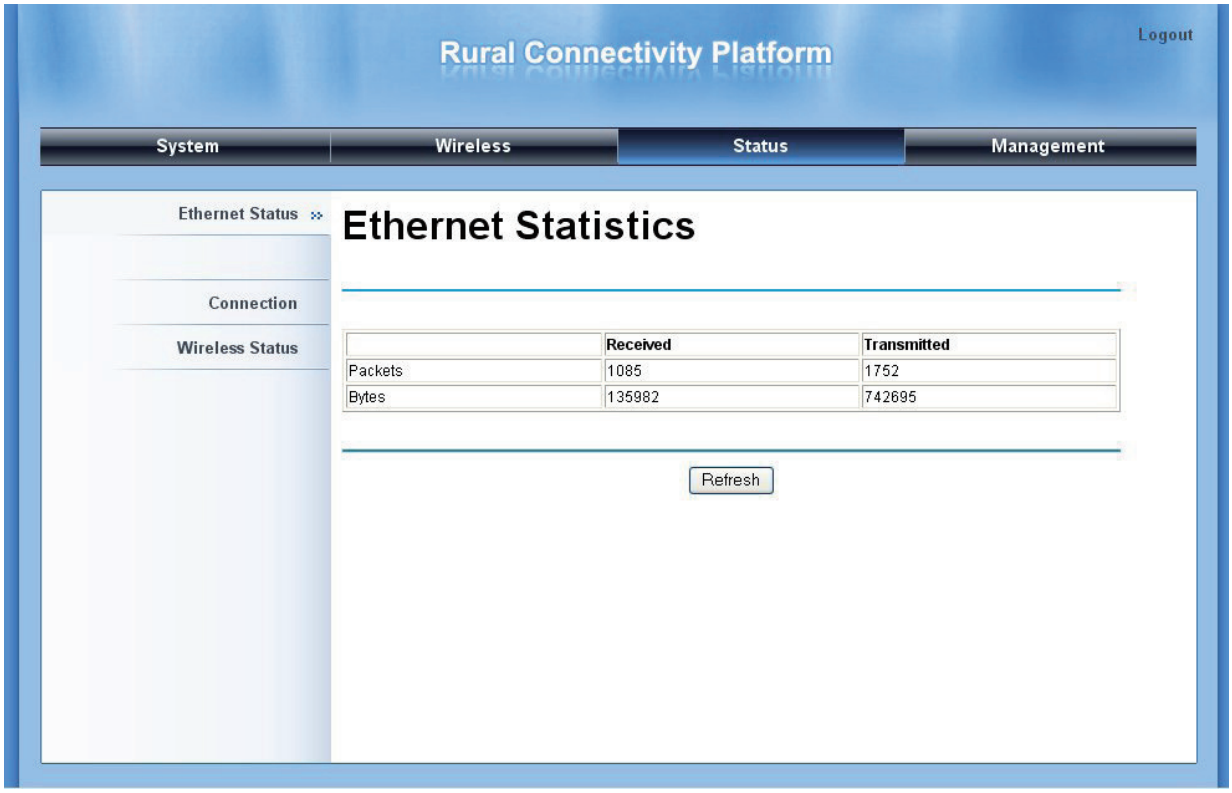


Figure 34 Ethernet Statistics

View Wireless Statistics

Open “**Wireless Status**” in “**Status**” to check the data packets received on and transmitted via wireless network. Click “**Refresh**” to view current statistics. All is read only.

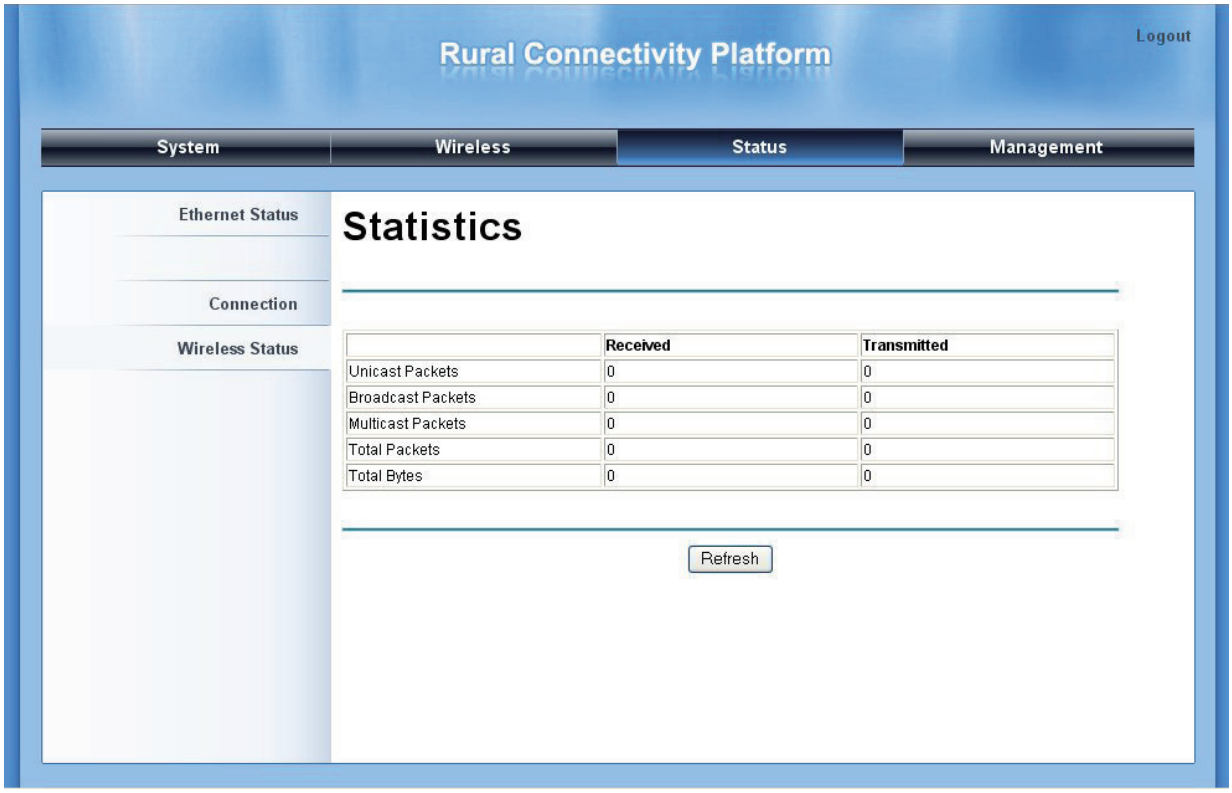


Figure 35 Wireless Statistics

Connection

Open “**Connection**” in “**Status**” to check the information of remote CPEs connected with bridge, these values also help determine whether the antenna is aligned in an appropriate direction. The table will be updated every 30 seconds. All is read only.

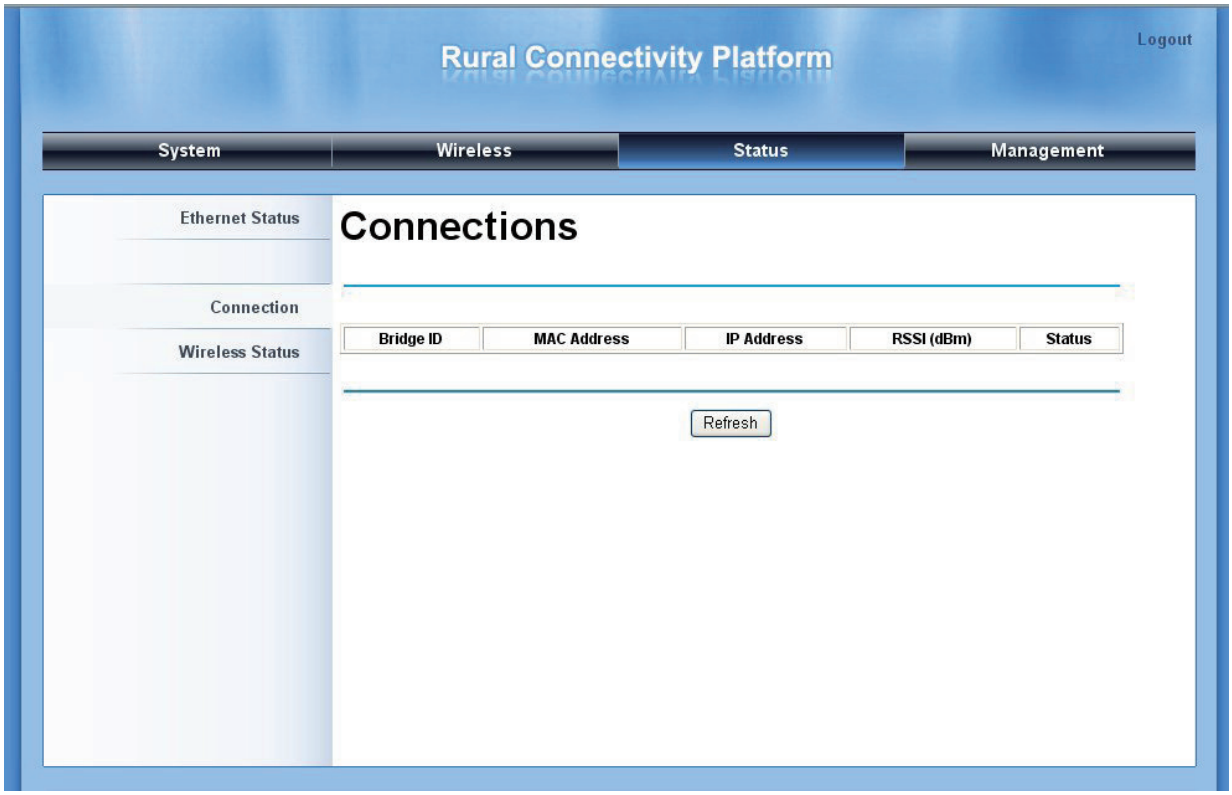


Figure 36 Connection

Password

From “**Change Password**” in “**Management**”, you can change or default the password to manage your R1 Extender.

Figure 37 Password

- **Change Password**

  For security concern, you have to enter the current password first and then enter the new one twice respectively in “**New Password**” and “**Repeat New Password**” fields.

- **Restore Default Password**

  If you would like to restore the default password, enter the current password first and then check “**Yes**” and click “**Apply**” to default the password.

Note:

- The password is case-sensitive and its length can not exceed 19 characters!

Remote Management

The R1 Extender provides you with two more options for device management, which are SSH (Secure Shell) and SNMP.

Open "**Remote Management**" in "**Management**" to configure the remote management of R1 Extender.

Figure 38 Remote Management

Remote Console

The R1 Extender supports CLI management, which could be accessed by Secure Shell (SSH). It is recommended PuTTY be used to login. Download it from http://www.putty.org/ for free. The minimum system requirement for using PuTTY is Windows 95, 98, ME, NT, 2000, XP and Vista on Intel x86.

Follow the steps below to implement:

- Once the program is downloaded, open up by double-clicking

. Note that before using PuTTY, be sure you are able to connect to the R1 Extender.
- Enter IP Address of R1 Extender (Default: 192.168.1.1), Port (22) and check SSH as connection

type;

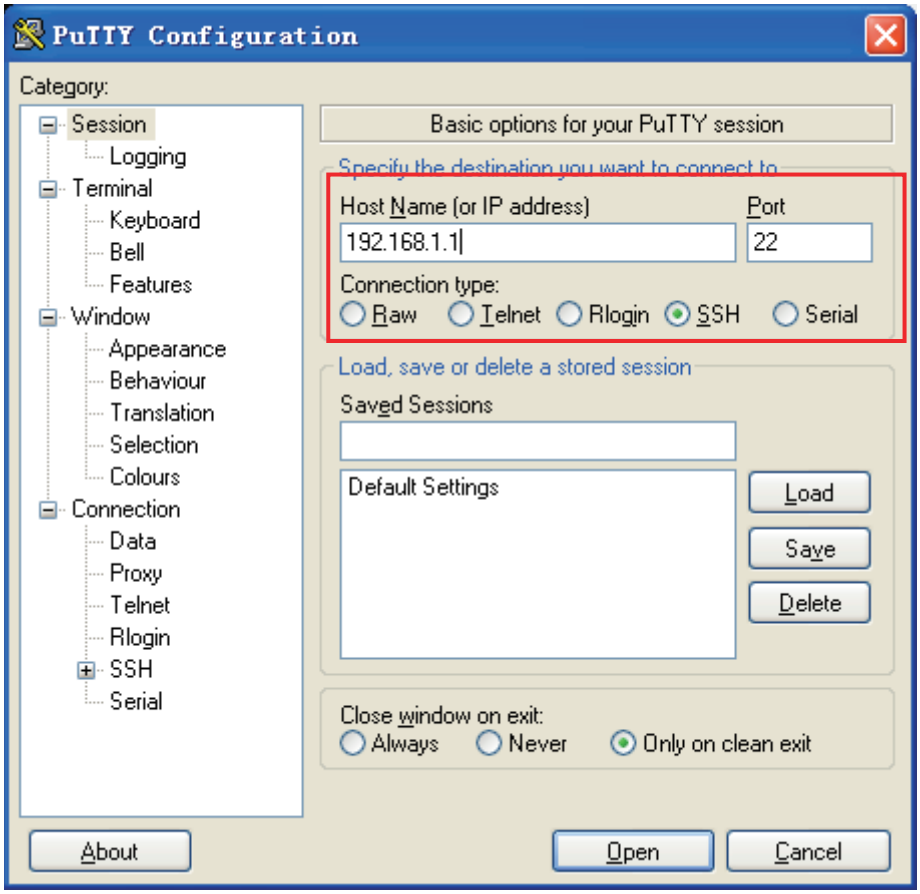


Figure 39 PuTTY Configuration 1

- From “**Connection**” in the left menu bar, click “**SSH**”; select “**2**” as “**Preferred SSH protocol version**”; make “**3DES**” the top position in “**Encryption cipher selection policy**”;

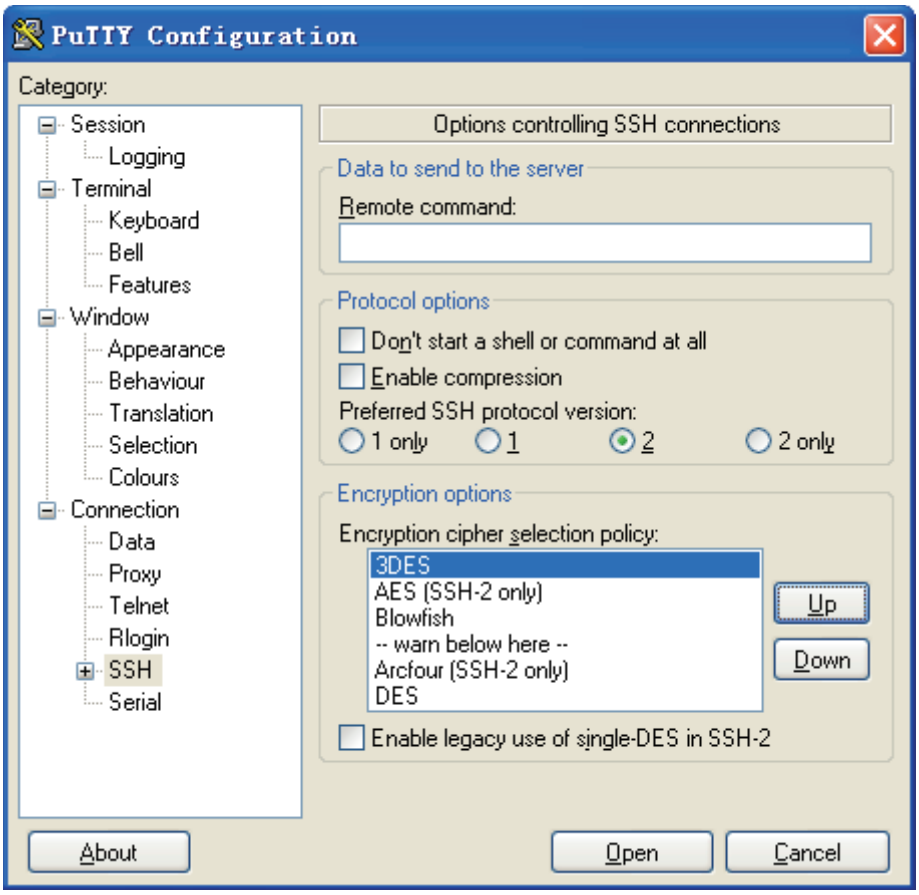


Figure 40 PuTTY Configuration 2

- Click “**Open**”, a window as below will popup:

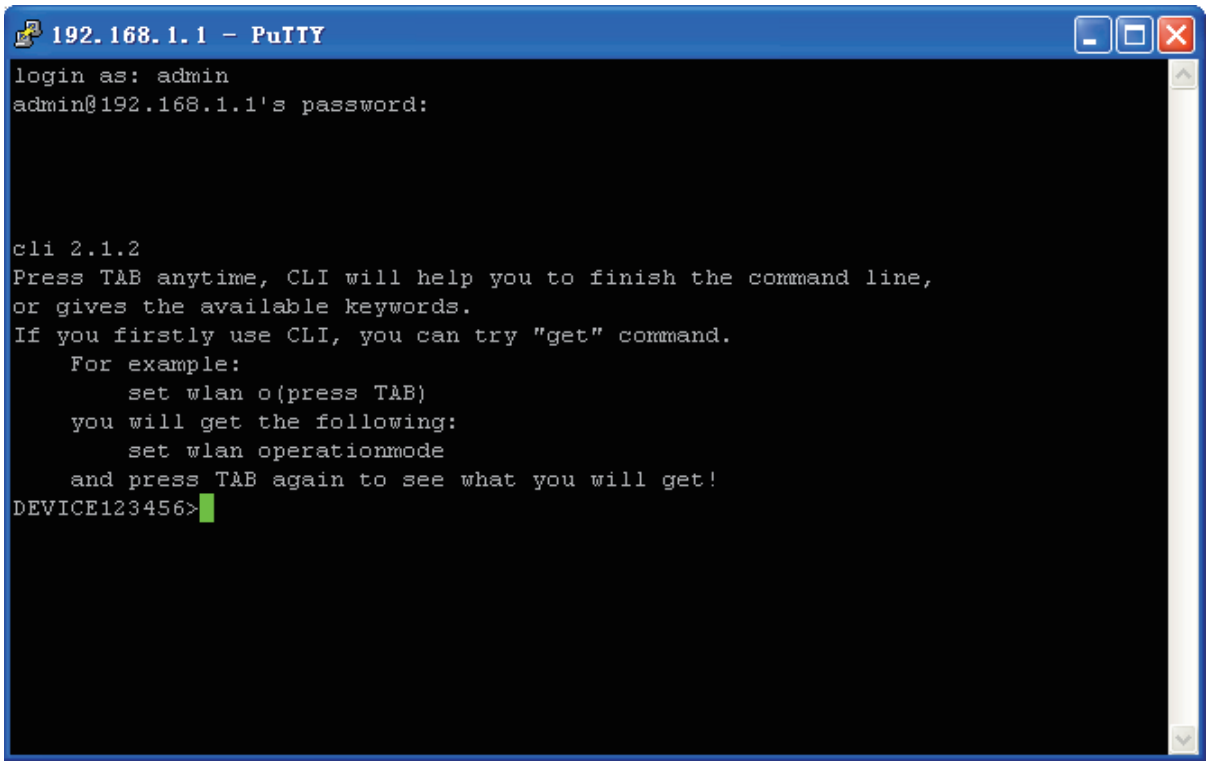

192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
cli 2.1.2
Press TAB anytime, CLI will help you to finish the command line,
or gives the available keywords.
If you firstly use CLI, you can try "get" command.
For example:
set wlan o(press TAB)
you will get the following:
set wlan operationmode
and press TAB again to see what you will get!
DEVICE123456>

Figure 41 SSH

- Enter the user name and password (Default user name/ password: admin/password) respectively, you will see "**DEVICE123456>**", which is the name of R1 Extender;
- Enter "**help**" command to get setting information; alternatively, you can refer to Appendix C. SSH Settings for details.

SNMP

The R1 Extender supports SNMP management. Set the SNMP parameters and obtain MIB file before remote management.

- From "**Remote Management**" in "**Management**", set the parameters for SNMP:
  - Enable SNMP by checking "**Enable**";
  - Specify the "**Read Community Name**", "**Write Community Name**" and "**IP Address to Receive Traps**"
  - Hit "**Apply**" to save settings.
- Obtain MIB file via FTP:
  - Enter ftp 192.168.1.1 , username (Default: **admin**) and password (Default: **password**);

- After successful login, enter command “**get bridge.mib**”, the information will as below and then bridge.mib file is obtained.

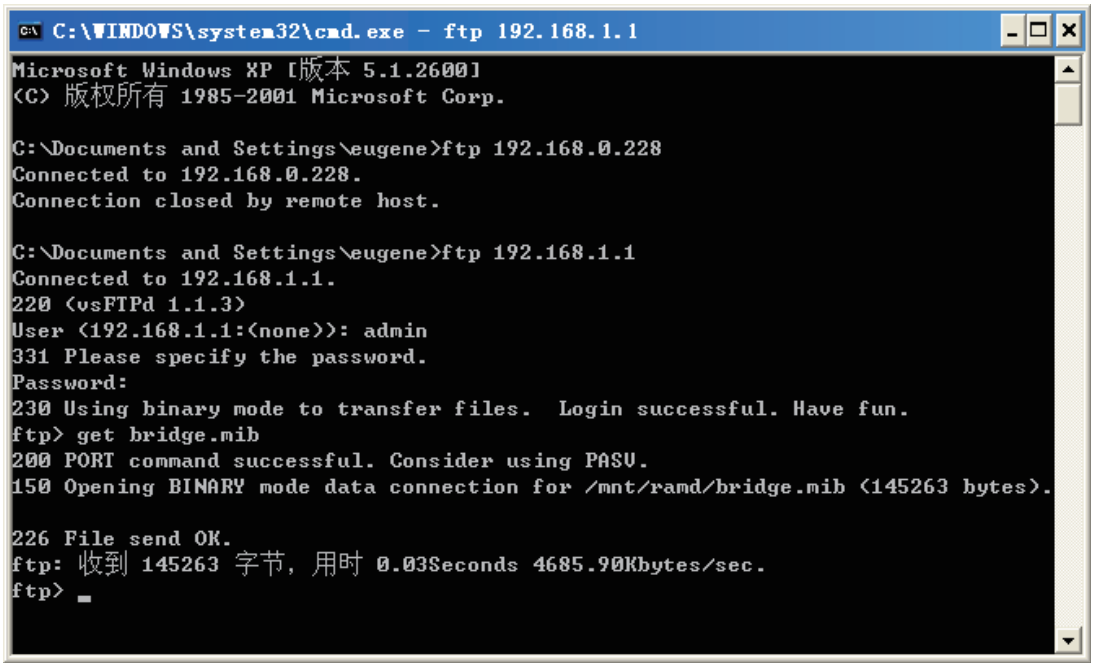

C:\WINDOWS\system32\cmd.exe - ftp 192.168.1.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\eugene>ftp 192.168.0.228
Connected to 192.168.0.228.
Connection closed by remote host.
C:\Documents and Settings\eugene>ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 1.1.3)
User (192.168.1.1:(none)): admin
331 Please specify the password.
Password:
230 Using binary mode to transfer files. Login successful. Have fun.
ftp> get bridge.mib
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for /mnt/ramd/bridge.mib (145263 bytes).
226 File send OK.
ftp: 收到 145263 字节, 用时 0.03Seconds 4685.90Kbytes/sec.
ftp>

Figure 42 Obtain MIB File

Time Settings

Compliant with NTP, R1 Extender is capable of keeping its time in complete accord with the Internet time. Make configuration in "**Basic**" from "**System**":

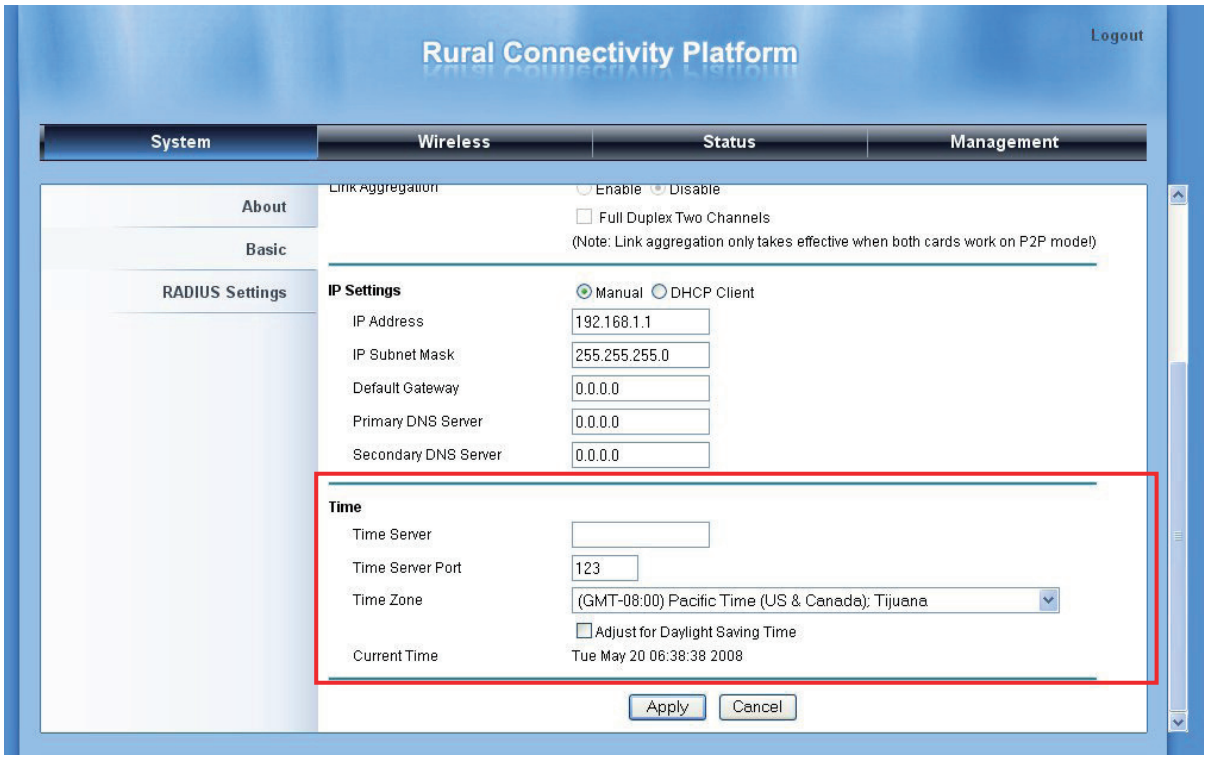
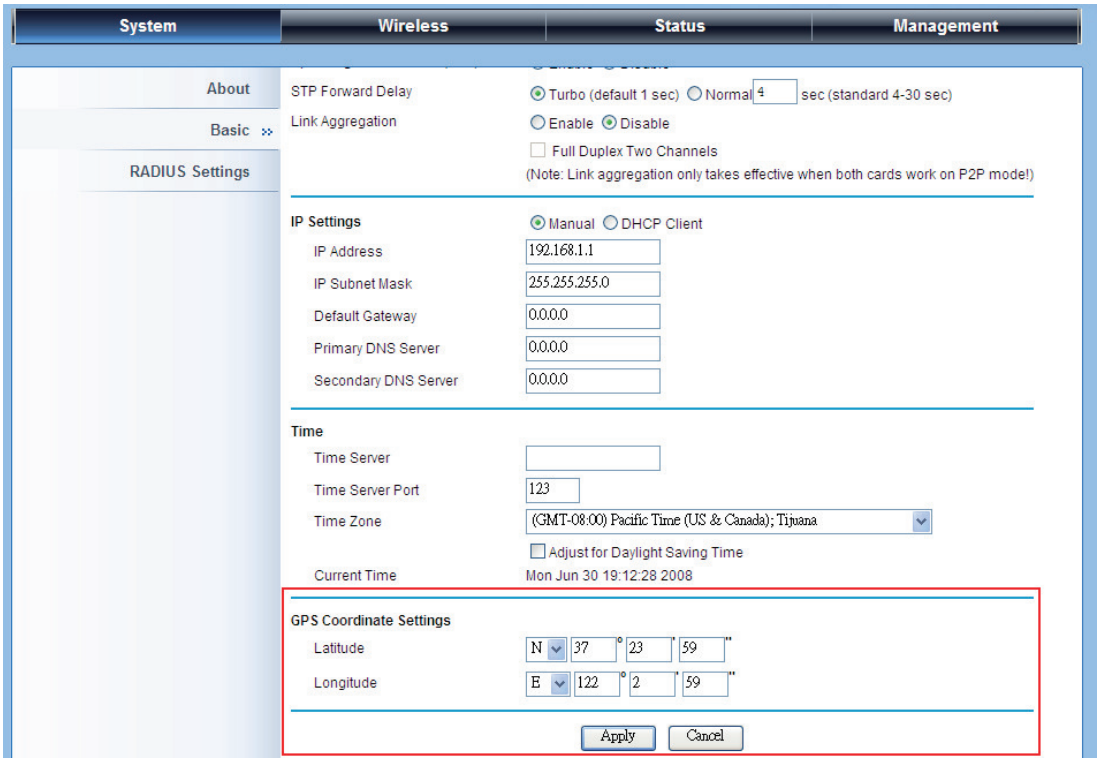


Figure 43 Time Settings

- Enter the time server IP address and port respectively in "**Time Server**" and "**Time Server Port**" fields;
- Select your desired time zone from the drop-down list, check "**Adjust for Daylight Saving Time**" if necessary;
- Hit "**Apply**" to save settings.

GPS Coordinate Settings

The GPS Coordinate Setting helps you mark the latitude and longitude of the R2E. From Basic in System, enter the coordinates and click the **Apply** button.



Upgrade Firmware

Open “**Upgrade Firmware**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through R1 Extender’s Web:

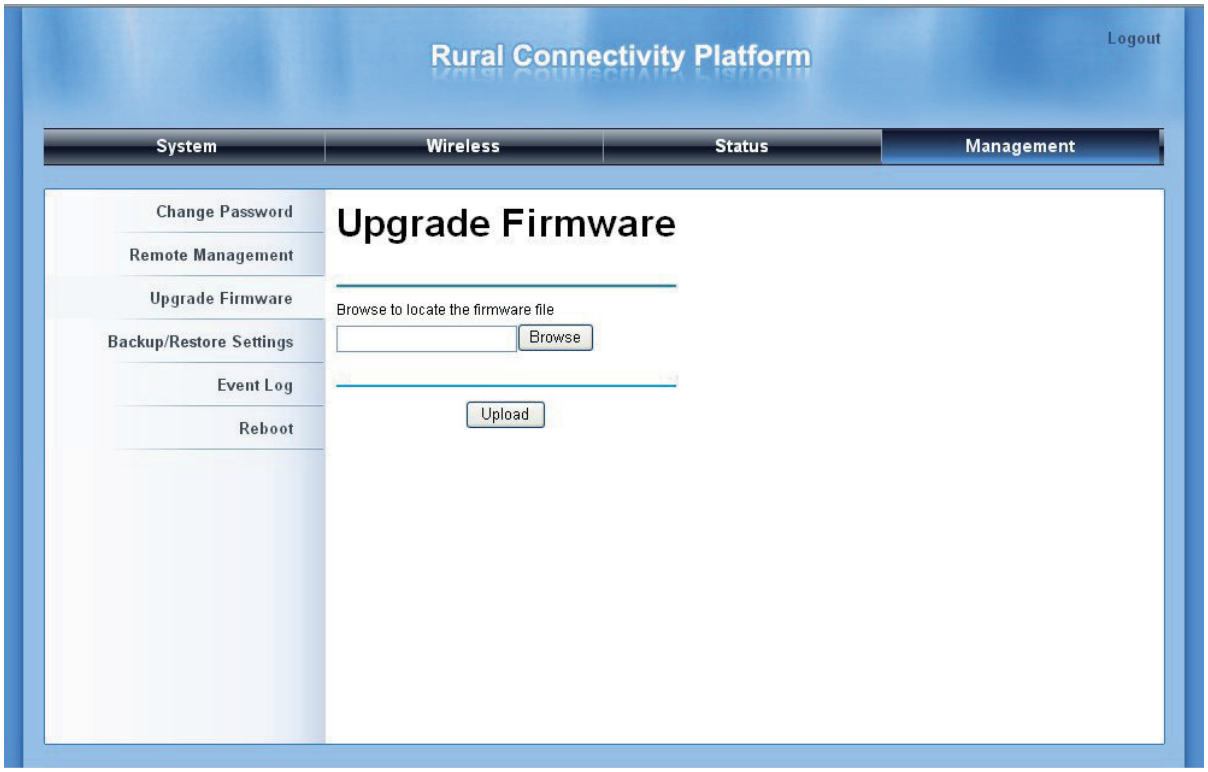


Figure 44 Upgrade Firmware

- Click "**Browse**" to select the firmware file;
- Click "**Upload**" to load the file into R1 Extender;
- Wait a moment, the system will reboot after successfully upgrade.

Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/Restore Settings

It is strongly recommended to back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "**Backup/Restore Settings**" in "**Management**" as below:

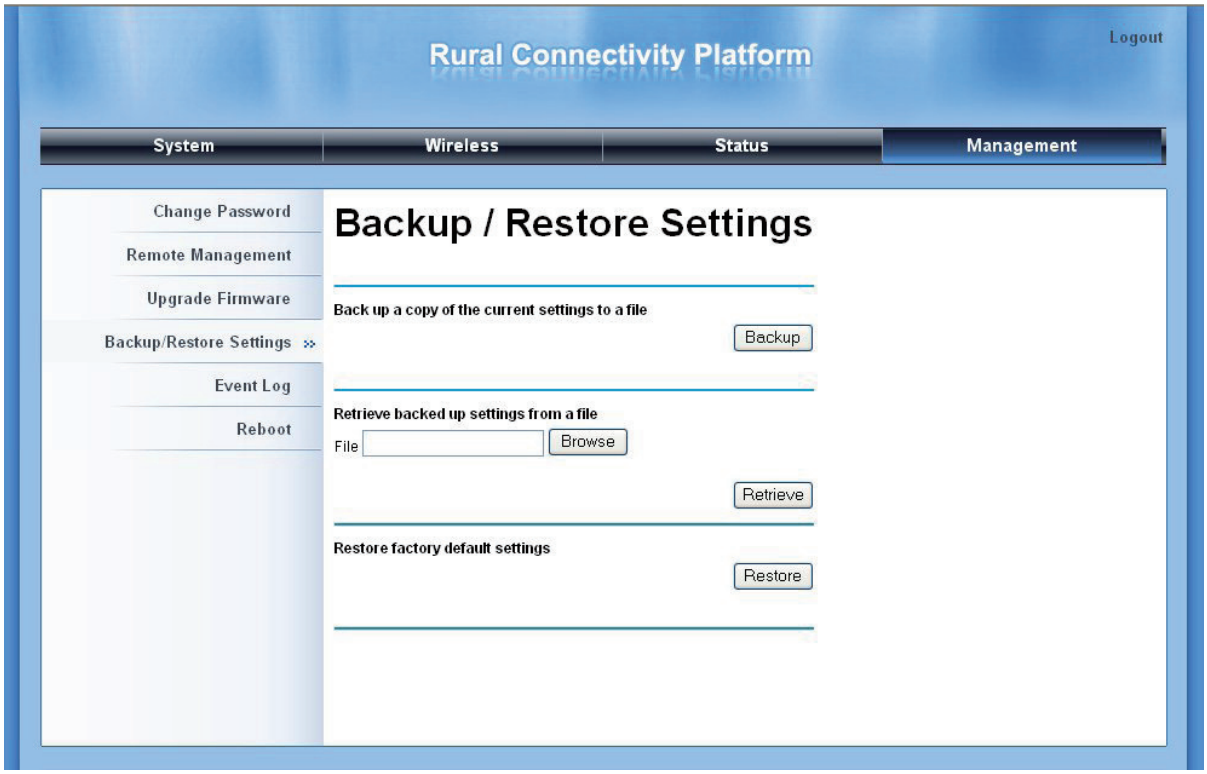


Figure 45 Backup/Restore Settings

- **Backup Settings**

  By clicking "**Backup**" a dialog box will popup. Save it, then the configuration file is saved to your local computer.

- **Retrieve Settings**

  By clicking "**Browse**" a file selection menu will appear, select the file you want to load, like bridge.cfg; Click "**Retrieve**" to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The R1 Extender provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**

  From “**Backup/Restore Settings**”, clicking “**Restore**” will eliminate all current settings and reboot your device, then default settings are applied.

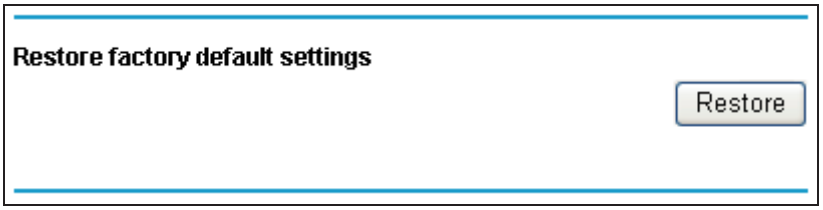


Figure 46 Restore Settings

- **Restore factory default settings via RS-232**

If software in R1 Extender is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via RS-232. For detailed instructions please refer to Chapter 2 RS-232 section.

Event Log

Event log is used for recording events occurred on the R1 Extender, including station connection, disconnection, system reboot and etc.

Open “**Event Log**” in “**Management**” as below.

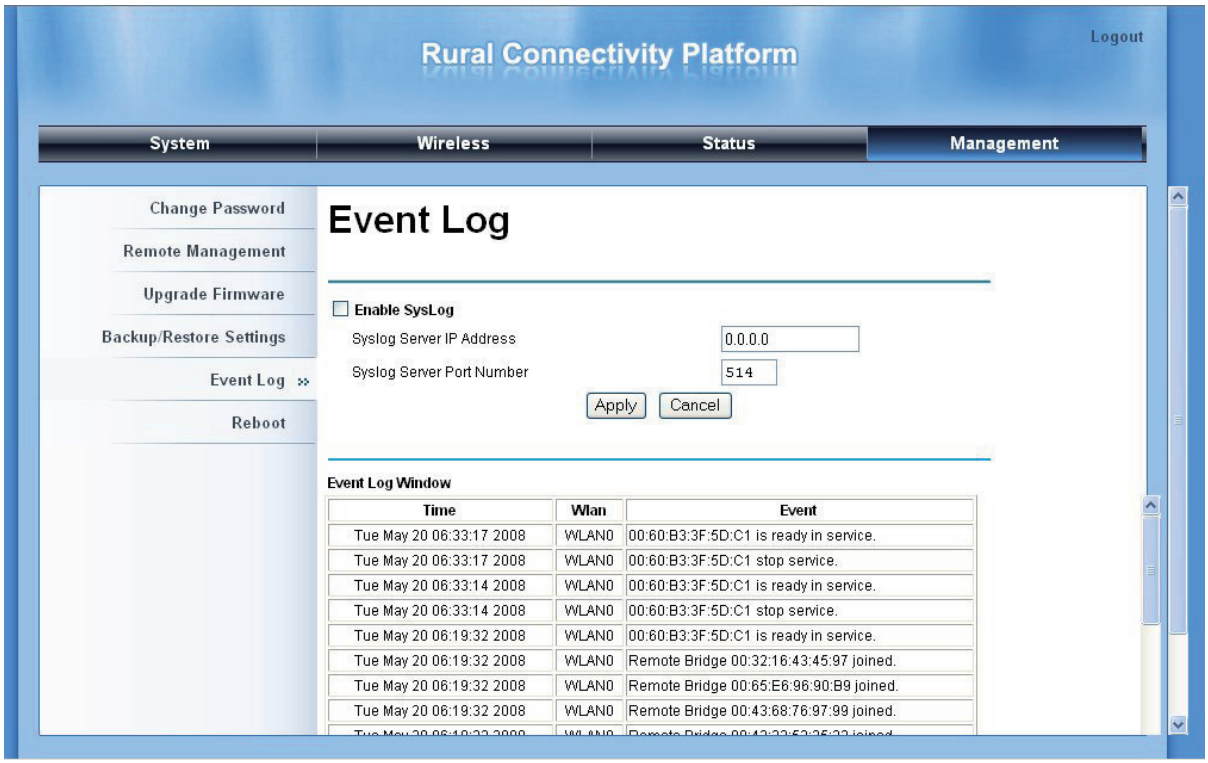


Figure 47 Event Log

- Enable Log: Enable System log or not;
- Syslog Server IP Address: Specify the IP address of the server;
- Syslog Server Port Number: Specify the port number of the server;
- Hit “**Apply**” to save settings;
- Event Log Window: Lists all occurred events in this field.

Reboot

You can reboot your device from “**Reboot**” in “**Management**” as below:

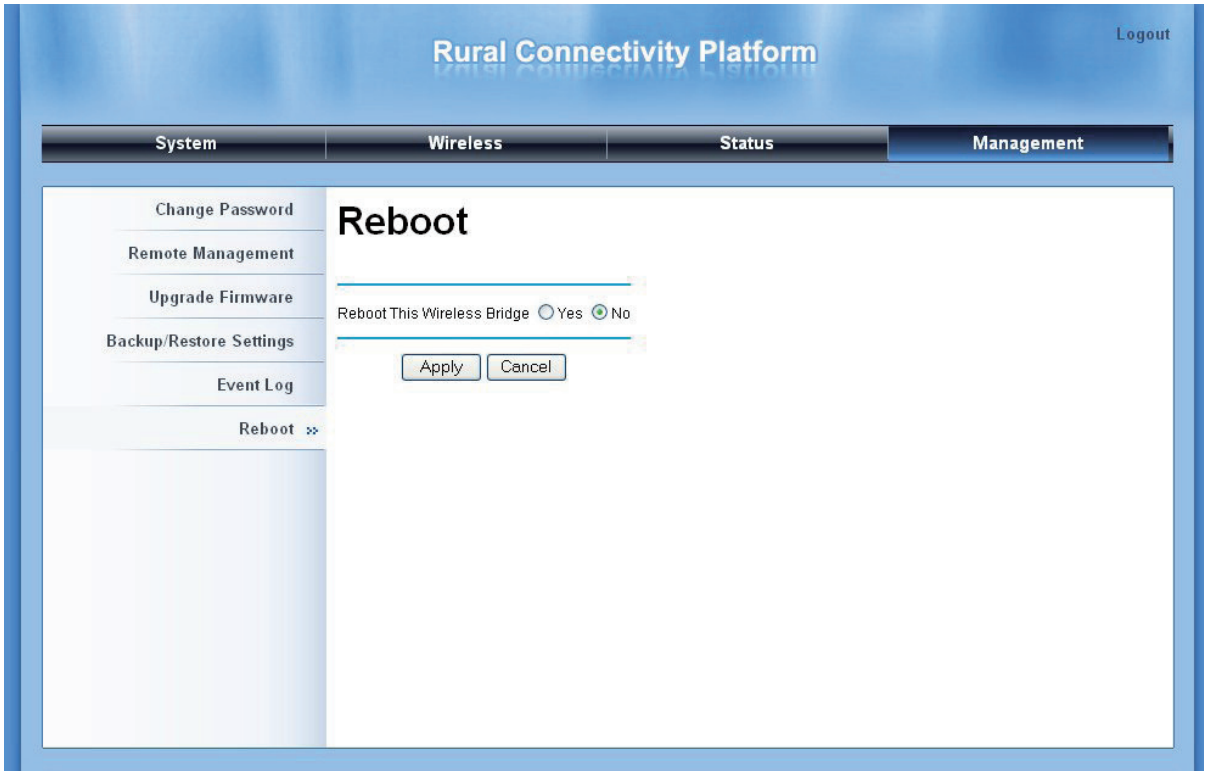


Figure 48 Reboot

- Check “**Yes**” and click “**Apply**” to reboot R1 Extender. This takes a few minutes, during which the device will send out the buzzing sound, informing you the system is rebooting.

Chapter 6 Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the R1 Extender. For warranty assistance, contact your service provider or distributor for the process.

Q 1. What if my R1 Extender fails to connect to the remote one?

- **Ethernet Link**: Check the availability of power to the bridge by observing the LED status on the power injector or on top of the RJ-45 Jack of the unit.
  - Green: The R1 Extender is connecting to the backhaul network.
  - Off: The R1 Extender disconnects from the wired network, check whether the power cord and Ethernet cables to the network and bridge are correctly connected.
- **Basic Configurations**: Mismatched basic settings among bridges are the most common cause of connectivity fail. If the bridge does not associate with a remote bridge, check whether options in each device are identical.
- **Security Settings**: Remote bridges attempting to authenticate to your bridge must support the same security options configured in your bridge, such as WEP and WPA (2)-PSK. If your bridge fails to associate with others, check whether the security settings are the same as your bridge settings.
- **Antenna Alignment**: If the methods above are all checked to be correct, you can observe and verify antenna alignment with RSSI value.

Q 2. What if I would like to reset the unit to default settings?

You may restore factory default settings in “**Backup/Restore Settings**” from “**Management**”.

Q 3. What if I would like to backup and restore my configuration settings?

You may do the backup by generating a configuration file or retrieve the settings you have backed up previously in “**Backup/Restore Settings**” from “**Management**”.

Q 4. What if I can not open the Web-based management interface?

Please check the followings:

- Check whether the power supply is OK; Try to power on the unit again.

- Check whether the IP address of PC is correct (in the same network segment as the unit);
- Login the unit via other browsers such as Firefox.
- Hardware reset the unit.

Q 5. What if the signal quality is poor or not so good?

- Check whether there is obstacle between units. Obstacle may lead to poor signal.
- Check the antenna height. Place the unit in a high position can help to get a better communication in long distance transmission.
- Check the polarization direction of antenna. Keep the polarization direction of antennas on two associating units the same; if not (one is horizontal, another is vertical), the signal quality may reduce dramatically.
- Check the antenna angle. Align the antenna to the remote one if using directional antenna. Big angle shift may lead to poor signal.
- Check the feeder length. Too long feeder may increase the signal loss and affect the unit performance.

Appendix A. Channel – Frequency Table

The R1 Extender can be operated in four different band widths, which are 5MHz, 10MHz, 20MHz and 40MHz. The following tables illustrate the channel with corresponding frequency in each band width.

Table 4 Channels in 5MHz Centre Frequency

Channel	Frequency
149	5.745 GHz
150	5.750 GHz
151	5.755 GHz
152	5.760 GHz
153	5.765 GHz
154	5.770 GHz
155	5.775 GHz
156	5.780 GHz
157	5.785 GHz
158	5.790 GHz
159	5.795 GHz
160	5.800 GHz
161	5.805 GHz
162	5.810 GHz
163	5.815 GHz
164	5.820 GHz
165	5.825 GHz

Table 5 Channels in 10MHz Centre Frequency

Channel	Frequency
149	5.745 GHz
151	5.755 GHz
153	5.765 GHz
155	5.775 GHz
157	5.785 GHz
159	5.795 GHz
161	5.805 GHz
163	5.815 GHz
165	5.825 GHz

Table 6 Channels in 20MHz Centre Frequency

Channel	Frequency
149	5.745 GHz
153	5.765 GHz
157	5.785 GHz
161	5.805 GHz
165	5.825 GHz

Table 7 Channels in 40MHz Centre Frequency

Channel	Frequency
149	5.745GHz
157	5.785GHz
165	5.825GHz

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Appendix B. Channel – Country List Table

The R1 Extender support country selection, there are different channel when select different country.

The following tables list the channel with country code in each bandwidth.

Table 8 Country of FCC

Country	Mode	Channel list			
		40Mhz	20Mhz	10Mhz	5Mhz
United States	11bg (1-11)	6	1/2/3/4/5/6/7/8/9/10/11	1/2/3/4/5/6/7/8/9/10/11	1/2/3/4/5/6/7/8/9/10/11
	11a (5725～5850)	149/157/165	149/153/157/161/165	149/151/153/155/157/159/161/163 165	149/150/151/152/153/154/155/156/157/158/159/160/161/162/163/164/165

Table 9 Country of European Union

Country	Mode	Channel list			
		40Mhz	20Mhz	10Mhz	5Mhz
Belgium	11bg (1-13) *Ukraine Excluded CH12-CH13	6	1/2/3/4/5/6/78/9/10/11/12/13	1/2/3/4/5/6/7/8 9/10/11/12/13	1/2/3/4/5/6/7/8 9/10/11/12/13
Bulgaria					
Croatia					
Cyprus					
Czech Republic					
Estonia					
Finland					
F.Y.R.O.Macedonia					
France	11a (5470～5725) Excluded CH120~CH131 Meteorology Radars	100/108/116 140	100/104/108/112 116/136/140	100/102/104/106/ 108/110/112/114/ 116/118/134/136/138/140	100/101/102/103/ 104/105/106107/ 108/109/110/111/ 112/113/114/115/ 116/117/118/119/ 133/134/135/136/ 137/138/139/140/ 141
Germany					
Greece					
Hungary					
Iceland					
Italy					
Latvia					
Lithuania					
Luxembourg					
Malta					
Netherlands					
Poland					
Portugal					
Romania					
Slovakia					
Slovenia					
Spain					
Sweden					
Turkey					
South Africa					
Nigeria					
Russia					
*Ukraine					
Austria					

Table 10 Other Countries

Country	Mode	Channel list			
		40Mhz	20Mhz	10Mhz	5Mhz
*Ireland Liechtenstein Norway Switzerland Denmark	11bg	6	1/2/3/4/5/6/7/8/9/10/11/12/13	1/2/3/4/5/6/7/8/9/10/11/12/13	1/2/3/4/5/6/7/8 9/10/11/12/13
	11a (5470～5725) Excluded CH120~CH131 Meteorology Radars	100/108/116/140	100/104/108/112/116/136/140	99/101/103/105/107/109/111/113/115/117/119/133/135/137/139/141	99/100/101/102/103/104/105/106/107/108/109/110/111/112/113/114/115/116/117/118/119/133/135/136/137/138/139/140/141
	(5725~5875) Excluded 5795~5815	151/167	147/151/155/167/171	146/148/150/152/154/156/158/164/166/168/170/172/174	146/147/148/149/150/151/152/153/154/155/156/157/158/164/165/166/167/168/169/170/171/172/173/174
	*Ireland Excluded 5795~5805	151/167	147/151/155/163/167/171	146/148/150/152/154/156/158/162/164/166/168/170/172/174	146/147/148/149/150/151/152/153/154/155/156/157/158/162/163/164/165/166/167/168/169/170/171/172/173/174

UK	11bg (1-13)	6	1/2/3/4/5/6/7/8/9/ 10/11/12/13	1/2/3/4/5/6/7/8 9/10/11/12/13	1/2/3/4/5/6/7/8 9/10/11/12/13
	11a (5470～5725) Excluded CH120~CH131 Meteorology Radars	100/108/ 116/140	100/104/108/112/ 116/136/140	99/101/103/105 /107/109/111/113 /115/117/119/133/ 135/137/139/141	99/100/101/102 /103/104/105/106 /107/108/109/110 /111/112/113/114 /115/116/117/118 /119/133/135/136 /137/138/139/140 /141
	(5725~5850) Excluded 5795~5815	151/167	147/151/155/167	146/148/150/152 /154/156/158/164 /166/168	146/147/148/149/ 150/151/152/153/ 154/155/156/157/ 158/162/163/164/ 165166/167/168/ 169

Appendix C. ASCII

WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 11 ACSII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

Appendix D. SSH Settings

Table 12 SSH Settings

get	set	del	Keyword				Descriptions
√	√		time				--time setting
√				-now			--current system time
√	√			-zone			--time zone
√	√			-daylight saving			-- daylight saving
√	√			-server			--time server setting
√	√				-name		--time server (domain name or IP address)
√	√				-port		--time server port
√	√		system				--system setting
√				-version			--system firmware version
√	√			-devicename			--system name
√				-macaddr			--system MAC address
√	√			-country			--country/region
	√			-restoreFactory Default			--restore factory default
√	√			-iptype			--system dhcp client
√	√			-ipaddr			--system IP address
√	√			-netmask			--system network mask
√	√			-gateway			--system gateway
√	√			-dns			--system dns
√	√				-primary		--primary system DNS server
√	√				-secondary		--secondary system DNS server
√	√			-stp			--enable spanning tree protocol
√	√			-ethrate			--ethernet data rate
√				-ethstats			--ethernet statistics
√	√		radius				--radius setting
√	√			-auth			--authentication radius setting
√	√				-primary		--primary
√	√					-ipaddr	--radius IP address
√	√					-port	--radius port number
get	**set**	**del**	**Keyword**				**Descriptions**
√	√					-secret	--radius secret string
√	√				-secondary		--secondary

√	√					-ipaddr	--radius IP address
√	√					-port	--radius port number
√	√					-secret	--radius secret string
√	√	√		-wpa			--wireless WPA setting
√	√				-reauthtime		--wireless WPA re-auth period(in seconds)
√	√				-keyupdate		--enable wireless WPA global update condition
√	√					-mode	--wireless WPA global key update condition
√	√					-interval	--wireless WPA global key update interval
√	√			-account			--account radius setting
√	√				-primary		--primary
√	√					-ipaddr	--radius IP address
√	√					-port	--radius port number
√	√					-secret	--radius secret string
√	√				-secondary		--secondary
√	√					-ipaddr	--radius IP address
√	√					-port	--radius port number
√	√					-secret	--radius secret string
√	√		ssh				--enable remote SSH access
√	√		snmp				--SNMP setting
√	√			-server			--enable SNMP agent
√	√			-trap server			--SNMP TrapServer IP address
√	√			-read community			--SNMP ReadCommunity
√	√			-write community			--SNMP WriteCommunity
√	√		log				--syslog setting
√	√			-client			--enable syslog client
√	√			-ipaddr			--syslog server IP address
√	√			-port			--syslog server port number
√	√		wlan				--wireless setting
√	√			-wirelessmode			--wireless mode
get	**set**	**del**	**Keyword**				**Descriptions**
√	√			-channel			--wireless channel(depends on country and wireless mode)
√	√			-txrate			--wireless transmission data rate

√	√			-bandwidth			--wireless bandwidth
√	√			-cpe mode			--use multicli or lan-to-lan
√	√			-cpedownflowwidth			--wireless down flow width for CPE mode
√	√			-OutputPower			--wireless transmit power
√	√			-VQoS/TDM			--enable TDM mode or not
√	√			-tdm timeslice			--station's timeslice value
√	√			-fragmentationthreshold			--wireless fragmentation threshold(even only)
√	√			-rtsthreshold			--wireless RTS/CTS threshold
√	√			-beaconinterval			--wireless beacon period in TU (1024us)
√	√			-operating mode			--wireless operation mode
√	√	√		-remotebs			--wireless remote AP(s)(depends on operation mode)
√	√	√			-pxp		--remote AP address for pxp mode
√	√					-wirelessisolate	--pxp wirelessisolate
√	√	√				-1	--1st remote AP for pxp mode
√	√	√				-macaddress	-- remote AP mac address for pxp mode
√	√					-bandwidth	--down flow width for pxp mode
√						-status	--remote AP status or active for pxp mode
√						-ipaddr	--remote AP ipaddr
√						-rssi	--remote AP rssi
√	√	√				-2	--2nd remote AP for pxp mode
√	√	√				-macaddress	--remote AP mac address for pxp mode
get	**set**	**del**	**Keyword**				**Descriptions**
√	√					-bandwidth	--down flow width for pxp mode
√						-status	--remote AP status or active for pxp mode
√						-ipaddr	--remote AP ipaddr
√						-rssi	--remote AP rssi
√	√	√				-3	--3rd remote AP for pxp

							mode
√	√	√				-macaddress	--remote AP mac address for pxp mode
√	√					-bandwidth	--down flow width for pxp mode
√						-status	--remote AP status or active for pxp mode
√						-ipaddr	--remote AP ipaddr
√						-rssi	--remote AP rssi
√	√	√				-4	--4th remote AP for pxp mode
√	√	√				-macaddress	--remote AP mac address for pxp mode
√	√					-bandwidth	--down flow width for pxp mode
√						-status	--remote AP status or active for pxp mode
√						-ipaddr	--remote AP ipaddr
√						-rssi	--remote AP rssi
√	√	√		-acl			--wireless access control
√	√				-mode		--enable wireless access control(ACL)
√	√	√			-list		--display trusted CPEs
		√				-all	--(delete only)all local ACL address
√	√	√				-(null)	--edit local ACL address
√				-association			--list of associated wireless clients
√				-wlanstats			--wlan statistics
√	√	√		-key			--wireless wep key setting
√	√				-type		--wireless wep key type
√	√	√			-1		--wireless wep key 1
get	**set**	**del**	**Keyword**				**Descriptions**
√	√	√			-2		--wireless wep key 2
√	√	√			-3		--wireless wep key 3
√	√	√			-4		--wireless wep key 4
√	√			-spaceinmeter			--wireless space in meter
√	√	√		-remotebssid			--wireless remote bssid in cpe mode
√	√			-remotessid			--wireless remote ssid in cpe mode
√				-network-status			--wireless network status
√				-bsscanlist			--bs list
√				-signal level			--signal level(dBm)

√				-remoterssi			--remote bs and rssi
√	√			-wmm			--wmm settngs
√	√			-super_audio			--Fast_Frame settings
√	√			-super_video			--super burst settings
√	√			-super_picture			--compression settings
√	√	√		-bs			--<null>
√	√				-ssid		--network name of this bs(1-32 chars)
√	√				-hiddenssid		--bs ssid broadcast suppress
√	√				-wirelessisolate		--bs isolate communication between clients
√	√				-authentication		--bs authentication type
√	√				-encryption		--bs data encryption
√	√				-default		--bs wep default key index
√	√	√			-psk		--bs pre-shared key(PSK) for WPA-PSK or WPA2-PSK
√	√			-autowdsenable			--auto wds settings
√	√			-wdsgroupid			--wds group id name
			password				--system password
			reboot				--reboot system
			exit				--logout from CLI
			quit				--quit CLI

Appendix E. GPL Declamation

PUBLIC SOFTWARE DECLAMATION

In the software we delivered, there are may contain some public software, if it is, please read below carefully:

1. Definition

"Public Software", when applicable, shall mean that portion of the Licensed Software, in source code form, set forth in the below Table, and provided under the terms set forth in the Section 5, the indicated website, the complete license terms can be found .

"Public Software" shall mean each of:

(a) any computer code that contains, or is derived in any manner (in whole or in part) from, any computer code that is distributed as open source software (e.g. Linux) or similar licensing or distribution models; and

(b) any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software (i) be disclosed or distributed in source code form, (ii) be licensed for the purpose of making derivative works, or (iii) be redistributable at no charge.

Public Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (1) GNU's General Public License (GPL) or Lesser/Library GPL (LGPL); (2) the Artistic License (e.g., PERL); (3) the Mozilla Public License; (4) the Netscape Public License; (5) the Sun Community Source License (SCSL); (6) the Sun Industry Source License (SISL); and (7) the Apache Software license.

2. Limited Use

Any Public Software provided under the agreement shall be subject to the licenses, terms and conditions of its model. Licensee hereby agrees to comply with the terms and conditions applicable to any such Public Software, as set forth in its presentation on website.

3. Limited Liability

The supplier hereby express that the supplier shall have no liability for any costs, loss or damages resulting from Licensee's breach of the terms and conditions applicable to use, conversion or combination of the licensed software with or into Public Software.

4. NO WARRANTY.

This program or licensed software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY. THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH LICENSEE.

5. Public Software Name and Description

Table 13 Public Software Name and Description

Program Name	Copy Right Description	Origin Sour Code	Licenses or Distribution Models or its special license terms	License Terms Website Reference
Redboot	Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.	ftp://ftp.ges.redhat.com/private/gnupro-xscale-030422/redboot-intel-xscale-030630.tar.Z	eCos License	http://sources.redhat.com/ecos/ecos-license/
Busybox		http://www.busybox.net/downloads/busybox-1.01.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
brctl	Copyright (C) 2000 Lennert Buytenhek	http://nchc.dl.sourceforge.net/s	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.ht

		ourceforge/bridge/bridge-utils-1.0.6.tar.gz		ml
dropbear	Copyright (c) 2002-2006 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu	http://matt.ucc.asn.au/dropbear/dropbear-0.51.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
hostapd	Copyright (c) 2002-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/hostapd-0.4.8.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
wpa_supplicant	Copyright (c) 2003-2005, Jouni Malinen <jkmaline@cc.hut.fi> and contributors	http://hostap.epitest.fi/releases/wpa_supplicant-0.4.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
mtdutil		ftp://ftp.uk.linux.org/pub/people/dwmw2/mtd/cvs/mtd/util/	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
ntpclient	Copyright 1997, 1999, 2000, 2003 Larry Doolittle	http://doolittle.icarus.com/ntpclient/ntpclient_2003_194.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
procps	Author: Albert Cahalan, Michael K. Johnson, Jim Warner, etc.	http://procps.sourceforge.net/procps-3.2.7.tar.gz	GNU GENERAL PUBLIC LICENSE Version 2 GNU LIBRARY GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html http://www.gnu.org/licenses/old-licenses/library.html
vsftpd	Author: Chris Evans	ftp://vsftpd.beasts.or	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-li

		g/users/cevans/vsftpd-1.1.2.tar.gz		censes/gpl-2.0.html
linux		ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.20.3.tar.bz2	GNU GENERAL PUBLIC LICENSE Version 2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html